PROJECT DELIVERABLE REPORT

DELIVERABLE NUMBER	D5.4
TITLE	DATA SHARING POLICIES
AUTHOR(S)	M.ALLIGIER, W.PINXTEN, L.STEVNER, M.PINART, C.ROUSSEAU, F.MATTIVI, A.HODGE, A.ASSPOLLU, R.CANALI & M.LAVILLE
WORK PACKAGE	WP 5
TASK	TASK 5.4
WP LEADER	M.LAVILLE
BENEFICIARIES CONTRIBUTING TO THE DELIVERABLE	CRNH, UHASSELT, UCPH, MCD, FEM, ULG, BIOCC, CRA-NUT
STATUS – VERSION	FINAL - VERSION 1.0
DELIVERY DATE (MONTH)	M24
SUBMISSION DATE	M30
DISSEMINATION LEVEL – SECURITY*	PU
DELIVERABLE TYPE**	O

* Security: PU – *Public*; PP – *Restricted to other programme participants (including JPI Services)*: RE – *Restricted to a group specified by the consortium (including JPI Services)*; CO – *Confidential, only for members of the consortium (including JPI Services)*

** Type: R – *Report*; P – *Prototype*; D – *Demonstrator*; - O - *Other*

CONTENTS

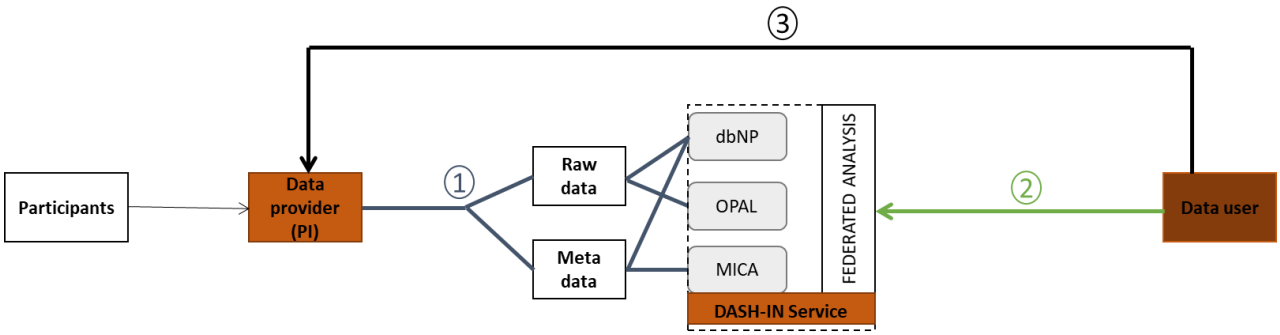
1- INTRODUCTION

ENPADASI aims to develop a database (WP3) based on the reuse of data obtained from different nutritional & clinical studies in Europe. However, the sharing of raw, meta or aggregated data raises several regulatory questions. Therefore, the scope of the WP5 is to define general rules required to share and reuse data in accordance with legal and ethical aspects of the EU participating countries and with respect to national policies. Four different topics are concerned in the WP5: ethics, data protection, data sharing polices and intellectual property.

Therefore, the deliverables of work package 5 aim to provide a set of rules and tools applicable to secondary use of nutritional data in the framework of ENPADASI project. Indeed, all the data users/providers have an obligation to operate in conformity with the requirements of their institution, and fulfill all necessary regulatory and ethical requirements imposed by their own national legislation.

Through several conference calls and one meeting in Paris, the consortium of the WP5, which gathers together several ethical & data protection experts, has identified the main ethical and data protection requirements to data sharing and has also proposed solutions and tools in order to help future data providers and users of the ENPADASI infrastructure to share and reuse their data in accordance with the current legislation.

2- DATA FLOW WITHIN THE ENPADASI INFRASTRUCTURE AND IDENTIFICATION OF THE DATA PROTECTION & ETHICAL ISSUES



Overview of the database architecture/data flow

1. It will be mandatory for the Data provider (see for definitions below in the definitions paragraph) to upload his metadata either in the MICA server or in the Phenotype database (www.dbnp.org). The data provider also has the possibility to upload his raw data on the Phenotype database or in an OPAL service. The metadata will be accessible within the ENPADASI consortium, thus each partner will be able to see which kind of study/data could be re-used. The data provider has also the possibility to upload the raw data of clinical studies (both interventional and observational) on the Phenotype database or the OPAL system. But contrary to the metadata, the raw data will not necessarily be

disclosed to the ENPADASI consortium. Each data provider will have the choice to restrict (even to only one data user) or open access to its raw data.

2. The data user can query the MICA server to identify studies of interest according to his scientific hypothesis. Thanks to the FEDERATED ANALYSIS tool, it will be possible to conduct a preliminary statistical analysis in order to validate or disprove the scientific hypothesis. The results of these statistical analyses are named aggregated data. The use of the FEDERATED analysis tool solves several ethical and data protection issues, allowing the future data user to combine the data and obtain statistical results without access to raw data, encountering ethics-related data-sharing concerns.

3. However, in order to go further and to publish the research from the combined analysis, access to the raw data will be mandatory. Two possibilities: the data user will contact the data provider directly, or the data user can have an access by the dbNP or OPAL server. The raw data access will raise several ethical and data protection issues that should be solved before use.

3-SHARING DATA THAT HAVE ALREADY BEEN OBTAINED

The Informed Consent Form (see deliverable 5.1) and related Participant Information Form offer opportunities to arrange the sharing of data. In some cases, it is explicitly stipulated in the informed consent process that gathered data can be stored and shared, for example for future research in the same pathology. In this case, data can be shared according to what has been specified in the participant information and informed consent form, in so far this is respectful to the applicable national and supranational law.

In practice, however, data sharing is not always anticipated as often informed consent procedures are ignorant of the issue. In these cases, consent must be regarded as specific to the project that is consented for, and implicit agreement to use data for future research cannot be presupposed.

Restrictions on data sharing no longer hold when data are fully anonymized, which enables data sharing. Anonymization, however, puts strong limits on data sets. As all connections between the data and the subject have been irreversibly broken, there is no way gather additional data (e.g. by gathering additional parameters retrospectively from patient records). In addition, shared data cannot be traced back to their original sources, which makes data sets vulnerable for pollution, in case mistakes or fabricated data would slip into the data sets. This could generate serious issues related to scientific quality and integrity.

4- SHARING DATA THAT ARE COLLECTED PROSPECTIVELY

When data are collected prospectively, data sharing can be anticipated proactively. In this case, the informed consent and related participant information can be used to specify how data sharing is arranged. A broad informed consent is helpful to enable data sharing (see deliverable 5.1). However, certain ethical issues need to be addressed when such a broad informed consent is put into place, and we recommend that following issues be anticipated:

- The kind of data will be stored and shared;
- How participants can withdraw their consent, and what happens with stored data when they do so;
- How long data will be stored;

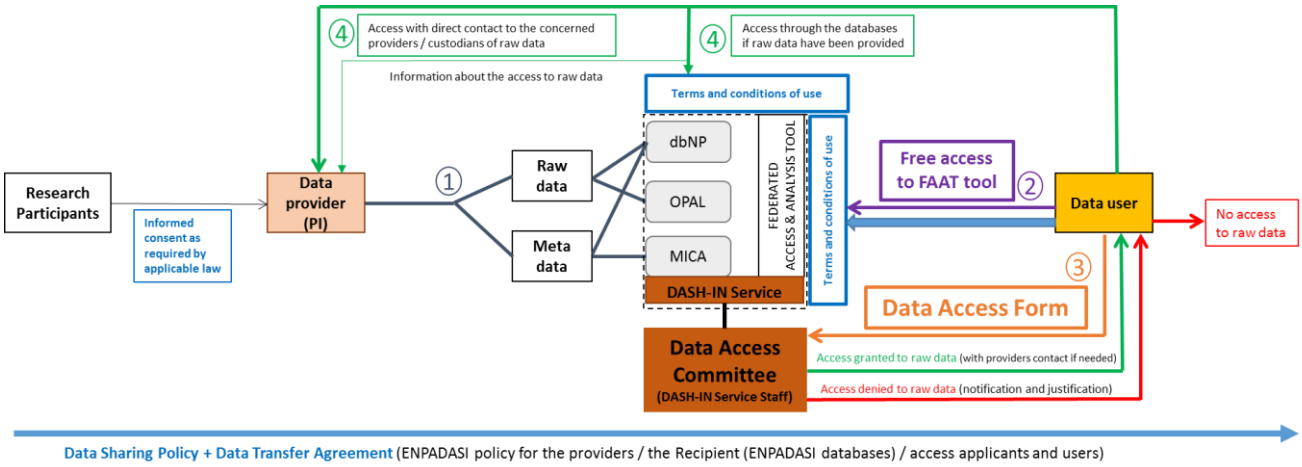
- What kind of research the data can(not) be used for;
- Whether/which individual research results will be fed back to the participant, e.g. when a finding of potential clinical relevance for the research participant is made in the course of data analysis;
- Whether or not there is a way for research subjects to know in what research their data are being used.

In addition, with the new GDPR-regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/) entering into force within a year, we recommend explicit referral to this regulation in the informed consent procedure.

5-DATA SHARING POLICIES

The Data Sharing Policy represents the framework in which the Data Providers inscribe in order to responsibly make available research data falling in the scope of Nutritional researches. The Data Users accessing the data made available through the database shall also conform to this policy in their activities with the accessed data.

This policy fixes general principles to be further detailed within other documents applying for accessing the database for research processing purposes (e.g. DTA for Data Providers and Terms and Conditions of Use for Users).



Proposed data sharing policies for the DASH-IN service

1) 'Data sharing' includes the provision of both studies' metadata (open access) and raw data (control-based open access) generated in research projects to the central database that will maintain them available for access by different users (through the DASH-IN Service) in the respect of this policy, of any restrictions fixed by the data provider in accordance with participants (data subjects) consent and other relevant legal and ethical frameworks.
2) The data user has a free access to the Federated Access and Analysis tool. Through this tool, he will be able to make preliminary statistical analysis on combined data sets without a direct access to raw data. However, before the utilisation of the DASH-IN service, the data user has to adhere to the terms and conditions of use of the tool.

3) To go further, and to access to the raw data the data user has to fill in a data access form and to send it to the data access committee. The data access committee will be in charge of the review of the data access form and to check if all the regulatory issues have been complied and the potential specific restriction of the data provider.
4) A data transfer agreement has to be signed by the data user before any access to the raw data. Two options for the data user to have access to the raw data :
    a. Throughout the ENPADASI tools, if the raw data have been uploaded
    b. By contacting the data provider

5.1) DATA ACCESS COMMITTEE

The DAC seeks to ensure that the data access applicant (the User) willing to process the raw data provides adequate protection with regard to the ENPADASI Data Sharing Policy principles, the provisions of this DTA, and in compliance with their domestic law, European and International laws and relevant guidelines in the concerned field of research and presents sufficient guarantees for ensuring responsible data sharing and use. In this mission, DAC members will ascertain the adequacy and consistency of the access requests: with the applicant qualifications, authorisation and ethical approval obtained; of the methodology presented as regard to the purpose of the study; and with regard to any restriction indicated by the Provider, in particular those arising from research participants consent or program specific restrictions. While the DAC is not an Ethics Committee, it should be entitled to assess the ethical, legal issues related to an access application that would arise and undertake further evaluations, if necessary in cooperation with the Provider.

5- DEFINITIONS

Anonymous/ised data: Information which does not relate to an identified or identifiable natural person and personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, including through cross-analysis by overlapping data.

Data Access Committee (DAC): Integral component of the DASH-IN Service for managing access to the data. The DAC is responsible for reviewing, approving or disapproving applications from potential users for a variety of restricted access cases.

Data Provider: The Provider (or 'Data Provider') is the individual researcher or investigator or body of researchers or investigators that makes data available for access and use within the context of the ENPADASI consortium and database. (It does not refer to the research participants.). The data provider should be the legal person or body that is responsible (owns) the data.

Data User: The 'Data User' is the individual researcher or investigator or body of researchers or investigators from either academia or industry that requests access to samples and/or data and use through the Data Sharing In Nutrition (DASH-IN) Service. The Data User is a 'data processor' in the meaning of the EU General Data Protection Regulation. The Data User may seek access outside of the context of the DASH-IN Service environment.

Ethics Committee: The term 'ethics committee' in this document refers to a committee which has given ethics approval for a study which has/intends to collect and use health data that will be

subsequently made available by the Data Provider within the database and the DASH-IN Service. (It does not refer to the ENPADASI Data Access Committee.)

Metadata: Metadata is data describing other data. Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier. Metadata can be created manually, or by automated information processing. Manual creation allow is the user to input any information they feel is relevant or needed to help describe the file, which is very relevant for example for the description of the study design. Automated metadata creation can display information such as file size, file extension, when the file was created, who created the file and can also include the logs of the machine used to generate the data. Metadata are highly aggregated and generalised data. Metadata is most often anonymised data.

Personal Data: Any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The use of the term 'personal data' in this document covers sensitive categories of personal information as defined within the EU General Data Protection regulation data such as health data, biological and clinical data and the use of wellbeing data. Such data are particularly protected under privacy rules and secured management and access processes.

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.

Raw data: Raw data refers to any data object that has not undergone thorough processing, either manually or through automated computer software. Raw data may be gathered from various processes and IT resources. Most digital equipment does not record the raw data but immediately processes it through vendor-defined algorithms into a vendor-specific primary record while discarding the original signals recorded in the equipment. In this context, such primary record files will be seen as analogous to raw data.

Raw data is primarily unstructured or unformatted repository data. It can be in the form of files, visual images, database records or any other digital data. Raw data is extracted, analysed, processed and used by humans or purpose-built software applications to draw conclusions, make projections or extract meaningful information. The processed data takes the form of information. Raw data can include personal data in the meaning of Article 4 of the General Data Protection Regulation of the

European Union (Regulation (EU) 2016/679 [1]). In such a case the respect of applicable personal data protection laws will need to be ensured by the data providers and the users of the DASH-IN service. Raw data shall be pseudonymised before any exchange in order to ensure appropriate data protection.

Sensitive data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation.

ANNEX: TOOLS AND PRATICAL INFORMATIONS TO SHARE DATA IN THE FRAMEWORK OF ENPADASI

ANNEX A: DATA TRANSFER AGREEMENT

1) PARTIES

The undersigned, the Provider *X [fill in official name of legal entity that is authorized to enter into this agreement]*, a *[fill in type of legal entity, e.g. foundation, charitable trust, corporation (ltd. Inc.)]*, incorporated, organized and duly existing under the laws of the *[fill in appropriate jurisdiction]*, with its principal office at *[insert address]*, hereby legally represented by *[insert name of legal representative]*,

and

the Recipient Institution Y *[fill in official name of legal entity that is authorized to enter into this agreement]*, a *[fill in type of legal entity, e.g. foundation, charitable trust, corporation (ltd. Inc.)]* incorporated, organized and duly existing under the laws of the *[fill in appropriate jurisdiction]*, with its principal office at *[insert address]*, hereby legally represented by *[insert name of legal representative]*,

(and/or… *[Add any other party which is to be a party to the DTA in the same way than in the previous paragraph]*,)

Whereas, the Provider X is a *[e.g. principal investigator, researcher, hospital, a cohort]* established with the aim to facilitate research on its collection of data; ENPADASI Infrastructure is willing to provide access to data to facilitate the conduct of research by Data Users on certain Data made available by the Provider. The Provider is aiming to transfer certain Data to the database managed by the Recipient, both having agreed to be bound by the provisions set out in this Agreement.

2) SCOPE OF THE SUPPLY

The Provider agrees to provide to the Recipient the data described in Annex A of the present agreement. *[fill in precisely Annex A, where the provision is described]*.

[1] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

Annex A summarises the data that the Provider will make available to the Recipient in accordance with their approved project *[project reference number]*. The timeframe and methodology by which the data will be dispatched is also set out in Annex A.

The Provider agrees to systematically provide study metadata but keeps a right to decide about the provision of raw data. Metadata shall be anonymised/ous data.

The Recipient acknowledges that the data are provided on an "as is" basis without any warranty of satisfactory quality or fitness for a particular purpose or use or any other warranty, express or implied.

3) DATA PROTECTION

The Provider remains vested of the data controller duties and rights fixed by the applicable national, European or international laws and regulations such as the EU General Data Protection Regulation and will be able at any time to restrict the use of the raw data provided based on legitimate grounds or to ask for a withdrawal of the data from the database. He is in charge of dealing with any complaints from data subjects and will remain solely responsible for the fulfilment of his legal and contractual obligations regarding the protection and sharing of data described in Annex A.

The Provider confirms that for the purposes of this DTA it is entitled to supply the data /and or personal data to the Recipient and that consent covering the intended use has been obtained from the relevant data subjects in compliance with applicable laws and/or guidelines.

The Recipient will be the data processor in charge of maintaining the databases and related access and analysis tool in application of this contract. The Recipient agrees to maintain a high level of data security and confidentiality and to cooperate with the Provider in order to ensure a legal, technical, organisational compliance as regards to the needs to ensure an efficient and sustainable data sharing infrastructure.

The Recipient will make the data available for further uses in research according to two different modalities:

- **Open access:** only regarding metadata. Open access refers to the practice of providing online access to scientific information that is free of charge to the end-user and reusable. This access is ensured by the DASH-IN Service and includes the free use of the Federated Access and Analysis Tool (FAAT) for pre-analytical purposes.

- **Restricted access:** regarding raw data, finest data, including potential personal data from research participants. The request from Users to access further data than those offered as open data must be performed using the Access Form (Annex 2). The request will be checked by the Data Access Committee (DAC) and then transmitted to the data providers for information and eventual argued refusal.

  Restricted access procedures to the raw data are envisaged as follows:

  Where raw data are provided to the database, the Recipient will consider any restrictions imposed by the Provider on datasets (Annex A) during the processing of Users access requests (Annex 2).

Prior to the access, the DASH-IN Service receiving access requests will review the Access Form and check whether the request is scientifically, legally and ethically grounded, whether the methodology is adequate and the purpose of the use fit with the datasets requested. As such the DASH-IN Service with take the role of the Data Access Committee (DAC) whose composition and role is further detailed in a dedicated section below.

Any request for access to raw data through the database from a potential Data User will be communicated to the Provider, with the corresponding Access Form and the Opinion from the Data Access Committee. The Data Provider keeps a right to refuse access to data on justification for 48 hours from the receipt of the data access documentation.

The access to raw data will be performed through the FAAT in a confidential and secured manner with adapted users' rights to the research purpose respecting in particular data minimisation.

Where raw data are retained by the Provider, metadata should indicate that further data are available on request from users. In such a case while there will be a prior DAC review of the application it will not suffice to grant access. Access applicants will need to directly contact the Provider who will then authorise access on his own responsibility. The Provider ensures the provision of relevant and sustainable contact details to the Recipient (Annex A) in order to relay such specific access requests. Parties agree that this situation should remain exceptional as it is complexifying data sharing.

Access applications may be refused by the Provider or the DAC. Reasons of refusal shall be notified to the other party and communicated to the access applicant.

In both cases of open and restricted access, the further use of the data shall limit to the purposes of the analyses set forth and within the limits set by the approved Research protocol and in the conditions specified in the Data Access Form only (Annex 2).

Where the Data User seek for reusing the data provided for another purpose than the initial one stated by the Provider and agreed by the data subject, the access will not be granted until formal, written and documented authorisation from the Data Provider. It pertains to the Data Provider to ensure that such reuses respect both data subjects' rights and applicable laws (e.g. through the practice of a purpose compatibility test and/or through the obtainment of an Ethics Committee special approval) as the Provider remain the main controller of the data provided.

The Data User accessing to the data via the FAAT will have to respect Terms and Conditions of Use (Annex 1) and confirm that the Approved Research Project has been subject to independent scientific review by a recognised body in the manner described in the Data Access Form and that the planned use of the data has approval of the appropriate ethics and scientific committees (Annex 2).

By accepting the terms and Conditions of Use the Data User will have to confirm that all work using the data will be carried out in compliance with all applicable laws, regulations, guidelines and approvals (Annex 1).

In this context, the Recipient, as well as the Data User, will retain the data in a secure network system at such standard as would be reasonably expected for the storage of valuable and sensitive/confidential/proprietary data.

The Recipient agrees to preserve, at all times, the confidentiality of information pertaining to identifiable individuals and other sensitive or proprietary information provided to the database. The Recipient agrees not to give access to data, in whole or part, or any identifiable data derived from the data, to any third party outside of the access through the DASH-IN Service and necessary processing related to management and maintenance of the IT system and databases.

Therefore, the Recipient shall limit access to and processing of the data to those employees or other authorized representatives of Recipient who: (i) need to process such data in order to conduct their work in connection with the data and the Protocol and (ii) have signed agreements with the Recipient obligating them to maintain the confidentiality of the data and any information to be derived thereof or disclosed to them.

The Recipient, as well as the Data User, shall refrain from tracing or identifying the identity of any data subjects who provided the data.

The Recipient, as well as the Data User, shall not attempt to contact any data subject.

The Recipient shall take reasonable steps to delete datasets for a given project on request from the Data Provider or individual data when the provider deems that the data subject has withdrawn his or her consent.

The Recipient confirms that it will deal promptly and appropriately with any withdrawals by data subjects which the Provider notify to the Recipient.

On reasonable notice to the Recipient, and in order to confirm or investigate compliance with the provisions of this DTA, the Provider may itself or via appropriate third parties:

- choose to inspect the premises and other relevant facilities of the Recipient and/or Data Users, in order to review the security, storage or other arrangements for the data ;
- request additional information about the data accesses (e.g. statistics) and related Approved Research Project and/or about the database progress as the Provider may, from time to time, reasonably require to the Recipient.
- the Provider will bear the costs of such audits unless a data default within the procedures and processes of the Recipient is discovered, in which case the Recipient will be obliged to reimburse the reasonable costs of the provider and any relevant third parties.

The same shall apply between the Recipient and the Data Users on decision from the DAC and as mentioned in the terms and conditions of use (Annex 1).

Any provisions of this agreement intended to protect the rights of human data subjects shall survive the expiry or termination of this agreement.

The Parties undertake to cooperate with the competent data protection authorities, particularly when they receive a request for information or in the case of an inspection.

4) DATA ACCESS COMMITTEE

The DAC is integrated to the central DASH-IN Service and will be ensured by qualified staffs in the field of scientific and statistical analyses, nutritional research, ethics and law.

The DAC shall be composed of a minimum of 2 professionals for providing a valid opinion. External expertise could be requested if necessary in the respect of confidentiality of the data.

The DAC is in charge of reviewing Data Access documentation in order to ensure fair access to the raw data made available by the Provider under the Restricted Access Procedure, whether they have been provided to the database or retained by the Provider.

In the context of the access application regarding available datasets that have been retained by the Provider, the DAC Opinion does not have the value of an access approval. The access shall be formally authorised by the Provider after a direct contact with the data user.

Where the data have been provided to the ENPADASI Database the Opinion form the DAC has the value of an access approval. Access to the data can be directly open to the user in 48 hours after the notification of the opinion to the Provider, if this latter does not oppose in this delay or keep silent.

The DAC seeks to ensure that the data access applicant (the User) willing to process the raw data provides adequate protection with regard to the ENPADASI Data Sharing Policy principles, the provisions of this DTA, and in compliance with their domestic law, European and International laws and relevant guidelines in the concerned field of research and presents sufficient guarantees for ensuring responsible data sharing and use. In this mission, DAC members will ascertain the adequacy and consistency of the access requests: with the applicant qualifications, authorisation and ethical approval obtained; of the methodology presented as regard to the purpose of the study; and with regard to any restriction indicated by the Provider, in particular those arising from research participants consent or program specific restrictions. While the DAC is not an Ethics Committee, it should be entitled to assess the ethical, legal issues related to an access application that would arise and undertake further evaluations, if necessary in cooperation with the Provider.

The DAC can reserve the right to audit Data Users' practices.

As a decision-making body the activity of the DAC is hereby approved. In case of conflicting views, the opinion of the Provider shall prevail on the DAC opinion and be respected. Such cases shall be recorded by the DAC Members and archived for accountability purposes.

5) INTELLECTUAL PROPERTY

Title to the data is and remains the ownership of the Provider and the data are made available to the Recipient as a service to the research community.

By providing the data, the Data Provider agrees to their reuse and cross-analyses in scientific research which could lead to marketable innovations and other intellectual creations.

The provision of the data and the availability of databases' content whether through open access or restricted access modalities as well as their use by the Recipient and Data Users, cannot be construed as conferring intellectual property rights (copyright, sui generis right) on these latter.

The Recipient and the Data Users shall be entitled to any inventions to the extent that these result from his own independent use of the data. The Recipient and Users shall grant the Provider a worldwide non-exclusive royalty-free irrevocable research licence with respect to any such inventions. If the Recipient and/or the User elects not

to seek any intellectual property protection with respect to such inventions he/they shall transfer any such rights to the Provider at no cost.

To the extent that the Provider and the Recipient have each contributed to an invention with respect to the data and/or database, they shall jointly own any rights to such an invention. Inventions made solely by the employees or agents of one party shall be owned by that party.

Except as expressly set forth in this Section, nothing herein shall be deemed to grant to either the Provider or Recipient any rights under the other party's patents, patent applications, trademarks, copyrights, trade secrets, know how (whether patentable or unpatentable) or other intellectual property rights.

Parties agree that the Provider can apply an embargo period of **6 months** for exploiting data and publishing research results before providing the data to the database.

6) RETURN OF RESULTS

The Provider and the Recipient agree that the Data User returns, at a time not before the date of publication of a paper that describes the results of any analyses of the accessed data, the following information/results for a publication via the Provider's and Recipient's website:

- General information about the analysis performed to inform the public.
- Summary data about the results to registered users of the Provider's and Recipient's website.
- A copy of any report of its results that derive from the use of the database to the Recipient and to the Provider in any format (e.g. paper journal, on-line report, meeting abstract).
- ….

Notices required under this DTA will be in writing and will be delivered by email to the addresses set out below or (in the event of a failure to deliver an email) by post to the Provider and the Recipient and will be deemed to be given, in the case of delivery by email, upon receipt at the addressee's email server (unless an automatic response indicating an undeliverable message is received) and, in the case of delivery by post, on the date of delivery (or, if not a business day, on the first business day thereafter).

Provider contact for reporting:

Email:

Postal address:

Recipient contact for reporting:

Email:

Postal address:

7) CREDITS AND PUBLICATIONS

The Data User shall agree to acknowledge the source of the data in any publications or other public disclosures reporting use of it. The following form of words should be used: "We acknowledge ENPADASI Infrastructure, funded by [..], and THE PROVIDER, funded by [..] for the supply of the Data [ref. of the dataset]".

The Data User, on the occasion of the publication of their research results, will use, if possible, the CoBRA guidelines[2] (citation of Bioresources in journal articles), in order to facilitate citation in the articles of datasets used in scientific research.

8) NOTIFICATION OF DATA BREACH

In case of data breach, for any reason, the Data User must immediately gather essential information about the breach and evaluate its impact on the data accessed and take appropriate measures to stop or diminish the impact of the breach and maintain data integrity.

The Data User shall without delay, and no later than 72 hours after having being aware of the breach, notify the Data Provider and the Recipient about the breach, as well as the competent Data Protection Authorities where mandatory, in particular according to the EU General Data Protection Regulation.

Data breach notifications shall also apply to the Data Provider as regard to the data provided to the Recipient and vice-versa.

Notification of Data Breach should be done using the form in Annex B. Contact details are provided in Annex B.

9) EXPIRY/TERMINATION

This agreement shall expire *[fill in date]*, unless earlier terminated by the mutual written agreement of the parties.

The Provider is entitled to terminate this DTA forthwith by written notice to the Recipient if:

- The Recipient commits any breach of a data provision of this DTA and, in the case of a breach capable of remedy, fails to remedy the same within 20 days after receipt of a written notice giving particulars of the breach and requiring it to be remedied. A breach will be considered capable of remedy if the Recipient can comply with the provision in question in all respects other than as to the time of performance, provided that time of performance is not of the essence.
- The Recipient PI ceases to be employed (or otherwise engaged by) the Recipient Institution; or
- The Recipient Institution ceases, is likely to cease, or threatens to cease carrying on business.
- The parties are facing an event of force majeure.

The rights to terminate this DTA given by this clause will be without prejudice to any other right or remedy of either party in respect of the breach concerned, if any, or any other breach.

On the Completion of the Research Project or on the termination of this agreement, the grant of rights to the Recipient will be automatically terminated and the Recipient will delete the data and confirm to the provider (in writing) that this has taken place.

10) CHARGES/PAYMENT

[2] http://www.bbmri-eric.eu/wp-content/uploads/2016/08/BBMRI-ERIC_ELSI_Services_CoBRA_V1.0_FINAL.pdf

In consideration for the Provider's entering into this Agreement, the Recipient agrees to pay the Provider an amount of [specify fee and VAT, if applicable] by wire transfer to the Provider, account Number [..], swiftcode [..].

This DTA is conditional on the Access Charges being paid and so, for the avoidance of doubt, no biodata/data will be provided to the Recipient until or unless the access charges are received in full.

11) ASSIGNMENT AND SUBCONTRACTING

Neither party will be entitled to assign this DTA or any of its rights or obligations hereunder without first having received the written approval of the other party, which approval not to be unreasonably withheld or delayed.

The Recipient will not subcontract the performance of any of its obligations under the DTA or any part thereof without having first obtained the prior written consent of the Provider, such consent not be unreasonably withheld.

In the event that consent is granted, the Recipient shall be responsible for the acts, defaults and omissions of its subcontractors as if they were the Recipient's own, and any consent given will not relieve the Recipient of any of its obligations under this DTA.

Data users accessing the data will need to mention any subcontractors ID, tasks and responsibilities in the Data Access Form (Annex 2). Any unplanned subcontracting will need to be priorly notified by written to the Recipient for consent. Depending on the nature and sensitivity of the data and of the subcontracted processing features, consent from the Data Provider will be asked. Any subcontractors will have to process the data in conformity with the highest data protection standards and in the respect of the ENPADASI Data Sharing Policy and other specifications provided by the Recipient of the Provider.

12) LIMITATION OF LIABILITY AND INDEMNITY

The Recipient will indemnify the Provider against all losses (whether direct or indirect, reasonably foreseeable or specifically contemplated by the parties), damages, costs, expenses (including but not limited to reasonable legal costs and expenses) that it incurs as a result of:

(i) the use, storage or disposal of personal data by the Recipient; or

(ii) any negligence or wilful default of the Recipient, provided that the Provider agrees to use its reasonable endeavours to mitigate any loss.

Both parties acknowledge and agree that the data are being supplied with no warranties, express or implied, and expressly disclaim any warranty of merchantability, fitness for a particular purpose, non-infringement or that the data will not degrade in recipient's safe keeping.

While best efforts will be deployed in order to ensure responsible use of the database, parties disclaim responsibilities as regard to any fraudulous or illegal uses of the dash-in service and related database by users. Will not infringe the patent or proprietary rights of any third party.

In no event shall either party be liable for any indirect, incidental, special or consequential damages arising out of or in connection with this agreement whether or not that party has been advised of the possibility of or is otherwise on notice of such possibility.

13) FORCE MAJEURE

If any party is prevented from, hindered or delayed in performing any of its obligations under this DTA by reason of a Force Majeure Event, such party will promptly notify the other of the date of its commencement and the effects of the Force Majeure Event on its ability to perform its obligations under this DTA.

If mutually agreed by the parties, then the obligations of the party so affected will thereupon be suspended for so long as the Force Majeure Event may continue.

The party affected by a Force Majeure Event will not be liable for any failure to perform such of its obligations as are prevented by the Force Majeure Event provided that such party will use every reasonable effort to minimise the effects thereof and will resume performance as soon as possible after the removal of such Force Majeure Event. If the period of non-performance exceeds 28 days from the start of the Force Majeure Event, then, the non-affected party will have the option, by written notice to the other party, to terminate this DTA.

For the purpose of this clause, Force Majeure Event means any event beyond the reasonable control of a party including, without limitation, acts of God, war, terrorism, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, fire, flood or storm. For the avoidance of doubt, strike, industrial action, failure of technology systems, third party insolvency and failure of the Provider or any other third party will not be considered to be Force Majeure Events.

The provisions of this clause will not affect any other right which either party may have to terminate this DTA.

14) APPLICABLE LAW

This DTA will be governed by and construed in accordance with the laws of *[insert appropriate jurisdiction]*.

15) DISPUTE RESOLUTION

In the event of a conflict between the parties related to the validity, the interpretation, execution and/or termination of this Agreement or of any of its clauses, shall be privileged in a procedure for setting the the dispute amicably through the mediation or conciliation or, where appropriate, arbitration proceedings.

In the event of the failure of an amicable settlement procedure or by means of arbitration, the…….. courts are competent.

16) GENERAL

This DTA governs the relationship between the parties to the exclusion of any other terms and conditions and, together with any other document referred to in this Agreement, constitutes the whole agreement between the parties in relation to the subject matter hereof. If there is any conflict between the provisions of this DTA and any of the annexes and related documents (including, but without limitation, the provisions of the Access Procedures) then the provisions of this DTA will apply.

A waiver, delay or forbearance by either party, whether express or implied, in enforcing or exercising any of its rights or remedies hereunder will not constitute a waiver of such right or remedy.

Special provisions of this DTA regarding rules to be applied under the umbrella of the Recipient to the future data users are intended to be enforceable by any data user who is not a party to this Agreement but that will bound to the Terms and Conditions of Use (Annex 1).

This DTA will create a collaboration based on agreed relationships between the parties.

All variations to this DTA must be agreed, set out in writing and signed on behalf of the parties before they take effect.

17) <u>ATTACHMENTS</u>

This Agreement incorporates the attached Annexes:

Annex A: Data Provision Form (for Provider only)

Annex B: Data Breach Notification Form (for Provider and User)

Annex 1: Terms and Conditions of use to which data users subscribe (opt-in) at the time of accessing the database (for User only)

Annex 2: Data Access Form (for User only)

ANNEX A: DATA PROVISION FORM

General: Annex A summarises the data that the Provider will make available to the Recipient in accordance with their approved Project and in compliance with the rules of this DTA. The Data Provider shall fill-in one Annex A per project. Extra-items can be added where necessary.

Data Supplier:

Data supply details:

- Source project title:
- Source project reference number (e.g. GA number):
- Studied Health/Nutritional Conditions:
- Nature and conditions of the data provided: (be clear and specific as much as possible)

Nature of the data	*Condition of the data*	*Restriction of Access*	*Restriction of Use*	*Project Source or ENPADASI Ref?*
e.g. raw data, metadata, research results, biological, genetic/genomic, clinical, social data, individual data	e.g. pseudonymous/ised, anonymous, anonymised, directly identiable	e.g. fully provided to dBNP, OPAL, MICA (Open Access Cases) available but not provided; provided for access only to certain members of a project consortium with embargo period from DD/MM/YYYY to DD/MM/YYYY (restricted access cases)	e.g no commercial use, no genetic research	

- Number of individuals concerned:
- Number of datasets:
- Identifiers for quotation in publications per datasets (to the attention of any users):
- Timeframe for the provision of the data:
- Sharing methodology:

Data hosting sites location

The Provider informs the Recipient that the Data will be hosted in authorised servers located in the following sites and country/ies: *[provide a complete list of the countries hosting the shared data servers including postal address and contact details].*

The Parties agree to inform each other in advance and without delay if data hosting sites' countries, legal entity or contact details are changed for getting consent from the other party.

Additional items and information (if any):

Date: *DD/MM/YYYY*

Data Provider or mandated Representative signature:

ANNEX B: DATA BREACH NOTIFICATION FORM

General: This form is to be used when data controllers need to report a data breach to the ENPADASI Infrastructure and concerned Data Provider.

It should not take more than 15 minutes to complete. Complementary notifications can also use the same form appropriately numbered.

If you are unsure whether it is appropriate to report an incident, you should contact: *[provide contact details]*

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, e.g. incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

Data Breach Notification:

Notifier ID: *Name of the organisation / Country*

Date of the notification: DD/MM/YYYY

Declaration number: (1 for the first one, 2, 3, 4 etc. for complementary notifications)

1. **Organisation details**

   (a) *What is the name of your organisation – is it the data controller in respect of this breach?

   (b) Please provide the data controller's ENPADASI registration number.

   (c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. **Details of the data protection breach**

   (a) * Please describe the incident in as much detail as possible.

   (b) * When did the incident happen?

   (c) * How did the incident happen?

   (d) If there has been a delay in reporting the incident, please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

(g) Does this breach has been reported to your competent National Data Protection Authority or to any other competent supervisory authority? Please, mention the name of the authority and date of notification

3. Personal data placed at risk

(a) * Datasets placed at risk (provide batch number where feasible)

(b) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

(c) * How many individuals have been affected?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the organisation about the incident?

(f) To what concerns the data accessed through ENPADASI and the DASH-IN Service is there any other kind of data that have been affected by the breach (other than personal data in the legal meaning)?

4. Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected datasets? Please provide details, attach relevant documentation.

(b) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has your organisation taken to prevent a recurrence of this incident (including guidelines or training of personnel)?

Sending this form

Send your completed form to: [email address] with 'Data breach notification form' in the subject field, or by post to: [postal address]

Please note that we cannot guarantee security of forms or any attachments sent by email

What happens next? When we receive this form, we will contact you within seven calendar days to provide a case reference number; and any useful information to diminish the impact of the breach or prevent further breaches.

Please, keep the ENPADASI Infrastructure aware of any advances related to inquiry about this breach by using the contact details provided above.

ANNEX 1: TERMS AND CONDITIONS OF USE FOR ACCESS TO DATA

Dear User.

You are accessing to the ENPADASI database.

By using the Platform and its related data and tools you recognize to have read, and understood and therefore to comply with these rules.

1. General Principles

The use of this open access Platform and related content including the use of the Federated Access and Analysis Tool, shall respect applicable laws and best practices in your country as well as the following terms and conditions of use. You will be accountable regarding any misuse of the data and tools accessed.

Data access request and use shall be adequate, relevant and limited to what necessary in relation to the purposes for which they are processed ('data minimisation').

Any breaches of data security or confidentiality must be reported immediately to the DASH-IN Service without delay (see the data breach notification form).

Examples of data security breaches include (but are not limited to):

- Access by any unauthorised person (i.e. has not signed Terms and Conditions of Use for the relevant data set);
- Sharing ENPADASI data with unauthorised persons;
- Failing to ensure sufficient data protection; such as a loss of login details
- Erasure, loss or alteration of the data

The user is responsible to comply with any other notification obligation regarding authorities, employer etc. as fixed in applicable laws and professional regulations.

2. Ethical guidelines in accessing to the ENPADASI databases

Researcher(s) requesting data must act in the respect of confidentiality and any other restrictions imposed by the Data Provider for the use of the data that will be provided by ENPADASI. Any data provided remains the property of the initial Data Provider and shall be used only for the purposes for which data access was granted.

For accessing to further detailed datasets, you need to fill in the Data Access Form *(insert link toward online version of the form)*. Data will have to be used only for the purposes of the research described in the Data Access Form and in the respect of applicable laws and regulations.

Access fees may apply to some, but not all, data access requests:

a. Approved "open access data" requests will be provided at no charge.

b. Other data access requests may require a processing fee, which will be explained to the applicant after the request is reviewed.

Data must be stored in a secure location with access limited to research team members only.

Research data accessed can be used for academic or practitioner educational purposes. Professors may request data to use in teaching undergraduate and graduate classes. Doctoral students can request data for developing their dissertations.

Academic researchers are encouraged to produce peer-reviewed articles as a way to increase the body of knowledge about nutritional health research within the academic community.

Research will not be used to denigrate ENPADASI Infrastructure or its components, or in legal proceedings.

The cooperation of ENPADASI will be acknowledged in all research produced as a result of such cooperation (see below, point 5).

For reports written in English, the researcher will email a one- to two-page executive summary of the report to xxxxxxx@xxxxx.xxx within one (1) month of publication.

If the report is published in a language other than English, the researcher will provide a one-paragraph summary in English within one (1) month of publication.

The use of the data set for commercial purposes or marketing is forbidden.

Communications and reports based on ENPADASI data must focus on benefiting the public interest and the health improvement of population. They must include a disclaimer stating that the views in the report reflect the researchers' opinions and are not intended to represent the position or policies of The IIA or The IIARF.

3. Data access modalities

All the data available in open access are contained in anonymous form in the databases and are accessed through the DASH-IN Service and the Federated Access and Analysis Tool.

Raw data access, including finest and potentially personal data strictly protected and confidential, is subject beforehand to the fulfilment of a special Data Access Form *(insert the link towards online form if any)* and authorisation.

4. Open data/access licensing

The open access to databases is ensured by the DASH-IN Service and includes the use of the Federated Access and Analysis Tool (FAAT).

Databases are made available through an Open Access license (Creative Common - CC-BY 4.0), if this is compatible with the initial terms of access of the database.

The CC-BY-NC 4.0 Licence - allow the user to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material.
- You may not use the material for commercial purposes.

- The licensor cannot revoke these freedoms as long as you follow the license terms.

5. Return of data

Any data generated through research permitted by the access to ENPADASI databases, must be returned to the source database to encourage ongoing use by the research community. The user is required to provide ENPADASI with a copy of all data collected and/or generated, to be archived for future use.

The Data User returns, at a time not before the date of publication of a paper that describes the results of any analyses of the accessed data, the following information/results for a publication via the ENPADASI and Providers websites:

- General information about the analysis performed to inform the public.
- Summary data about the study results.
- ….

The Data Users shall provide a copy of any report of its results that derive from the use of the database to ENPADASI in any format (e.g. paper journal, on-line report, meeting abstract).

Notices required under these Terms and Conditions of Use will be in writing and will be delivered by email to the addressees specified to you by ENPADASI (by email or postal sending).

In certain limited cases, the secure erasure of the original data provided through the DASH-IN service could be explicitly required by the DASH-IN managers.

6. Intellectual property rights and publication

Any publication using and permitted by the data is must be made in open access.

The users, on the occasion of the publication of their research results, will acknowledge the database by using the following quote: …….

The above quote can be completed by specific quotations as indicated during the process for accessing raw data. They shall be used as an independent complement of the above mentioned general quotation.

If relevant, we recommend the use of the CoBRA guidelines (citation of Bioresources in journal articles), in order to facilitate citation in the articles of datasets used in scientific research.

7. Auditing

On reasonable notice, and in order to confirm or investigate compliance with the provisions of these Terms and Condition of Use, ENPADASI may itself or via appropriate third parties:

- choose to inspect the premises and other relevant facilities of the Data User, in order to review the security, storage or other arrangements for the data ;
- request additional information about the data accesses (e.g. statistics) and related Approved Research Project and/or about the data processing progresses as it can be reasonably required to the User.

- the Data User will not bear the costs of such audits unless a data default within the procedures and processes is discovered, in which case the User will be obliged to reimburse the reasonable costs to ENPADASI and any relevant third parties.

ANNEX 2: DATA ACCESS FORM

By requesting access to the ENPADASI databases, you can have access to different databases, each one integrating different type of data (raw data, metadata…). Access to data requires to fill an access form in which is described the project and the reasons why you need access to particular datasets.

A wide range of resources is available through access to ENPADASI platform. All the data are obtained from different authorised nutritional & clinical studies in Europe.

Please use this form to request access to data managed by the ENPADASI Infrastructure. Completed forms should be emailed to xxxxxx@xxxxx.xx

Name and Scope of Project	
Name of Project	
Geographic Scope (country or regions to be covered)	

Lead Researcher—Name and Affiliations	
First Name/Given Name	
Family Name/Last Name/Surname	
Job Title/Designation	
Certifications	
Organization Affiliation	
Industry of Organization	
IIA Institute Affiliation (if applicable)	
Country of Residence	

Lead Researcher—Contact Information	
Email Address	
Telephone Number	

Complete Mailing Address	

Lead Researcher—Qualifications	
Experience Related to Nutritional Studies	
Main Previous Activities in the Field	
Main Previous Publications in the Field	
Academic Degrees	
Data Analysis Experience/Skills	

Other Researchers—Name and Qualifications	
Name, Qualifications, Tasks, Location	
Name, Qualifications, Tasks, Location	

Project Overview	
Start Date (DD/MM/YYYY)	
Expected Completion Date (DD/MM/YYYY)	
Access period whished (if different from the ones of the project) (DD/MM/YYYY)	
One-Paragraph Description of Project Objectives (50 to 150 words)	

Maximum number of persons expected to have access to the data	
Categories of recipients and location (Organisation, Country, Tasks)	
Primary Methods of Distribution (for example, download from institute website)	
Publication Planned (Yes or No)	
Do you confirm that the project has received any necessary authorisations / ethical approvals required under applicable law? *If yes, please, provide GA number or reference to the obtained official documents* *If no, please justify and detail the authorisations/approval to be obtained*	

Type of Data Requested	
Kind of datasets / ref	*Processing Purposes and Methodology, Processing Location and Responsible Person if different from the applicant*

Upon approval, the applicant will be granted access to the data, either directly through the database or with a contact with the relevant Data Providers where the specificity of the data requires specific contractual agreements or authorisations. In this latter case a contact from ENPADASI will inform and guide you.

An amendment to the original access form must be completed if any of the following changes occur during the research using accessed data concerned by your approved request:

- Significant extension of the project's scope ;
- End date ;
- New researchers need to access the data ;
- Change in institution ;
- If any additional data are required

This amendment shall be further detailed and notified to your ENPADASI contact person without delay for approval and guidance.

Proposals for access may be refused. Reasons for refusal will be notified to the access applicant.