Instructions for Data Processing

Based on the EU General Data Protection Regulation ("GDPR"), University of Oulu ("UO") as the Data Controller of its Northern Finland Birth Cohorts’ ("NFBC") Data and Material is entitled and obliged to make sure that its collaborators as the "Controllers" of the disclosed Material (referred to as "Recipients") comply with the rules set forth in the GDPR to protect and enable research participants’ privacy rights.

For this purpose, UO gives the following instructions to complement the existing agreements (Data or Material Transfer agreement, DTA, MTA) ("Agreement") that it has concluded with the Recipients.

NFBC Material is managed by the Infrastructure for Population Studies ("INFRA") at the Faculty of Medicine, UO.

1. DEFINITIONS

“Material” means data and/or samples disclosed to the Recipient for a specific “Project” based on a NFBC Scientific Committee decision and a separate “Agreement” between UO and Recipient.

“Data Protection Laws” means all applicable EU and national laws on personal data and human samples protection in force from time to time. Including but not limited to the Personal Data Act 523/1999, Act on the Openness of Government Activities 621/1999, Medical Research Act 488/1999, the EU General Data Protection Regulation ("GDPR" 679/2016), the Finnish Data Protection Act 2019 and the laws on professional secrecy, as applicable.


“Personal Data” means information relating to an identified or identifiable natural person (hereinafter “Research Participant”). 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 of 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.

“Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
“Recipient” is data processor or data controller of the Material.

“Cohort study” is a longitudinal data collection that belongs to the Northern Finland Birth Cohort’s Health and Wellbeing research programme (NFBC1966, NFBC1986, aging cohorts Oulu1935 and Oulu1945).

“Research participant” is a member of the Cohort Study.

2. GENERAL

UO is requested by Data Protection Laws to act diligently when giving access to its Material. It must give the Recipient written instructions for the Processing of Personal Data. The Recipient must comply with such instructions immediately after receipt. The instructions may also include information, guidelines, instructions and obligations related to data security, and technical and organizational measures. UO may amend, update and revise such instructions, if needed.

The information on the Project and its duration, the nature and purpose of the Processing, the type of Personal Data and categories of Research Participants are defined in the Agreement.

These instructions are binding and apply to Processing activities of Material by the Recipient, and complement the existing Agreements between UO and the Recipient.

3. ROLES AND OBLIGATIONS OF THE PARTIES IN THE DATA PROCESSING

UO is allowed to disclose its Material only to Recipients who provide sufficient guarantees of implementation of appropriate technical and organizational measures to meet the requirements of the Data Protection Laws, and to ensure the protection of the rights of the Research Participants.

The Recipients are allowed to process Personal Data for the purposes of the Project only in accordance with the Agreement and these or further Instructions given by UO.

3.1. TECHNICAL AND ORGANIZATIONAL MEASURES

The Recipient must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk to secure the data processing 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, and must comply with UO’s instructions and any updates of such instructions.

The Recipient must implement measures to ensure that persons acting under the authority of the Recipient and who has access to Personal Data, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they comply with the Agreement and these instructions.
3.2. RESEARCH PARTICIPANT’S RIGHTS

The Recipient must assist UO by appropriate technical and organizational measures, insofar as this is possible, to fulfil the UO’s obligation to respond to requests for exercising the Research Participant’s rights laid down in Data Protection Laws.

The Research Participant has a legal right to withdraw from the Cohort study. In such a case, UO requires that the corresponding Research Participant is excluded from the Project using Material.

The requests concerning exercising of Research Participant's rights may require that the Recipient assists UO with notifications and communications to the Research Participant; execution of the access rights of the Research Participant; rectification or erasure of the Personal Data, execution of restrictions of data Processing and/or the right to data portability, as set out in the Data Protection Laws.

3.3. DELETION OR RETURNING THE PERSONAL DATA

The General Terms of Access to the NFBC resources has the following provision on completion of project and returning research results:

On completion of the research project, the research team must return any remaining usable samples to the INFRA, if requested to do or unusable samples must be destroyed and UO must be notified of it in writing (INFRA, NFBCprojectcenter@oulu.fi). The data provided by UO must not be used anymore. All electronic copies of the data held by the research team must be deleted with the exception of copies needed for backing up work.

The research team must submit to UO any new data (“New Data”) generated from the Material upon completion of the project. The New Data means for example assay and analysis data from biological samples or modified variables from the data supplied with appropriate documentation. UO has the right to make the Results available for other researchers via the standard material request process, at a date agreed in the Agreement with the Recipient.

3.4. OTHER OBLIGATIONS

UO has the right to amend, supplement and update any instructions given to the Recipient for any reason and at any time.

The Recipient must respond to any notifications, reclamations and other communications related to the Processing of Personal Data by UO with no delay and at the latest within seventy-two (72) hours of UO’s contact or reference.

If the Recipient breaches, violates or neglects the provisions of these Instructions, and/or the Data Protection Laws, the Recipient’s liability is set out in the applicable provisions of the Agreement.
In addition, such breach, violation or negligence must constitute a substantial breach of the Agreement, in consequence of which UO has the right to resort to the remedies provided in the Agreement.

UO and the Recipients are obliged to comply with Data Protection Laws regardless of content of or changes made to the Agreement or these Instructions. In case there is a conflict between the Data Protection Laws and the terms and conditions of the Agreement or these Instructions, each of the Parties must have the right and obligation to comply with the Data Protection Laws and such actions of complying with the Data Protection Laws must not be considered as a breach of obligations under the Agreement or these Instructions.

To comply with the Data Protection Laws UO must have the right to prevent, interrupt or discontinue any processing of Personal Data, if UO decides that such processing of Personal Data would not be in accordance with the Data Protection Laws. In such situation, UO must not be liable for any claims or damages, which may result from such decision.