M-7-4 Practical guide for researchers on using sensitive data in Nordic countries

Tryggve Checklist on ELSI issues and GDPR compliance

Version 1.0 - 17 December 2019

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Introduction

Ethical, legal and social implications (ELSI) are topics that require close attention when dealing with human data. The Tryggve ELSI activity aims to assess and document requirements associated with cross-border sharing, moving, storing and/or processing of human data for research purposes. Key aspect of this task is to provide supporting information and expertise for Tryggve use case recipients as well as the research community at large.

The approach taken is to create a checklist of items that are required for conducting cross-border human data research. It is meant to be a tool to help such projects to be aware of the requirements and identify gaps in these areas for the particular research cross-border collaborations, as this is something we have observed that many projects struggle with. The checklist items fall into the following categories: Ethical reviews, Compliance with GDPR, and other considerations. There is a clarifications and comments section at the end with more information about the different sections of the checklist.

**Further information**

Antti Pursula, Niclas Jareborg

neic.no/tryggve

tryggve@neic.no

@NordicTryggve

**Tryggve Checklist on ELSI issues and GDPR compliance**

|  |  |
| --- | --- |
| **Cohorts / Datasets** | [***More information***](#_yt63ssxvks41) |
| List and number the cohorts/datasets that will be used in the project | |
|  | |
| **Ethical reviews and informed consents** | [***More information***](#_bpq99s6psmgd) |
| Has the project (or parts of the project) undergone **ethical review**? | * Yes * Yes, some parts of the project * No * Needs to be confirmed |
| * What are the *limitations of use* in the ethics approval, if any? List per cohort/dataset   + e.g. only for research on certain types of diseases, sharing only within certain geographical boundaries, etc. Alternatively, state if there are *no limitations.* | |
|  | |
| Have **informed consents** been collected from the research subjects?  *Note: The content of informed consents needed to be valid under different laws (e.g. GDPR or ethical legislation) might differ.* | * Yes * Yes, for some cohorts * No * Needs to be confirmed |
| * What are the *limitations of use* defined in the informed consent, if any? List per cohort/dataset   + e.g. only for research on certain types of diseases, sharing only within certain geographical boundaries etc. Alternatively, state if there are *no limitations.* | |
|  | |
| State the intended **research purpose** | |
|  | |
| * Is the intended research purpose **within the scope** of the *limitations of use* that is defined in the ethics approval(s) and/or the informed consent(s)? | * Yes * No * Needs to be confirmed |
| GDPR | |
| State the purpose of processing the personal data  [*More information*](#_psh82ctxwc8m) |  |
| Who are the data **controllers** of the personal data processed in the project?  [*More information*](#_99kys1cm36lg) |  |
| * If there are more than one controller of the personal data processed in the project, will the parties be joint controllers?   + Has a joint controllership agreement between the parties been established? | * Yes * No, separate for each cohort * Needs to be investigated * Yes * No, but it should be * Needs to be investigated |
| What is the **legal basis** for processing the personal data?  *State cohort/dataset for each type of legal basis*  [*More information*](#_iu07g55i2nxk) | * **Public interest**   Datasets:   * **Consent**   Datasets:  Are consents in compliance with the GDPR?  Datasets:   * **Other**, which? |
| What are the **exemptions for the prohibition for processing of special categories of data** (such as health and genetic data) under Art. 9 GDPR used?  *State cohort/dataset for each type of exemption.*  [*More information*](#_hn82lwtwh7mr) | * Scientific research   Datasets:   * Consent   Datasets:   * Needs to be investigated |
| Have **data processing agreements** been established between the data controller(s) and any **data processors**? *List processors and agreements established for each of these*  *Note: A data processing agreement has to contain the obligatory clauses specified in* [*Art 28.3 of the GDPR*](https://gdpr-info.eu/art-28-gdpr/)*. The agreement should also regulate the use of any sub-processors.*  [*More information*](#_7oerp1b5bm4i) | |
| * Needs to be investigated * Not relevant   Processors:      Agreements:      Agreements:      Agreements: | |
| Have **Data Protection Impact Assessments** (DPIA) been performed for the personal data?  *List DPIAs done and for which parts of the data.*  *Note: All Nordic Data Protection Authorities have identified that most types of research projects on health or genetic data require a DPIA.*  [*More information*](#_2fr0po3rt0gm) | |
| * Needs to be investigated * Not needed (unlikely) | |
| What technical and procedural safeguards have been established for processing the data?  [*More information*](#_fs49xt61fwq5) | |
|  | |
| What happens with the data after project completion?  [*More information*](#_hikcge64w28a) | |
| The dataset(s) will be deleted | Datasets: |
| The dataset(s) will be archived at the controller(s) | Datasets: |
| The dataset(s) will be archived in a controlled access repository for re-use.  *Note. Subjects should be informed about this, and that this should preferably be stated in the informed consents and/or ethical approvals.* | Datasets: |
| In what form will the data sets be stored? | * Irrevocably anonymised Datasets: * Pseudonymised Datasets: * Identifiable Datasets: |
| **Other considerations** | [***More information***](#_41zfj9xlczxf) |
| Are there other relevant national legislation considerations that has to be taken into account?   * e.g. regarding public access to information (in particular SE?), biobank acts, etc. | * Needs to be investigated * No * Yes: |
| Are there other Terms & conditions for data access (in particular if presenting obstacles for cross-border processing of health data)?   * e.g. register data access policies (requirement of PI in the same country, moving data to other secure services) | * Needs to be investigated * No * Yes: |
| Are there other legal agreements between use case parties that should be considered?   * e.g. conditions regarding data reuse and intellectual property | * Needs to be investigated * No * Yes: |

**Clarifications and comments**

### Cohorts / Datasets

This section provides a way to label each dataset with a number that can be used to refer to the dataset in other sections of the checklist.

### Ethical reviews and informed consents

The purpose of this section is to spell out, for all datasets, what uses the subjects have consented to, and/or for what uses ethical approvals have been given. Then, given the stated research purpose of this project, are the consents and ethical approvals for the datasets compatible with this.

### GDPR

#### State the purpose of processing the personal data

The GDPR stipulates that to process personal data the controller must do that with stated purposes, and not further process the data in a manner that is incompatible with those purposes ([Article 5 - Principles relating to processing of personal data](https://gdpr-info.eu/art-5-gdpr/)).

#### Who are the data controllers of the personal data processed in the project?

[Article 4](https://gdpr-info.eu/art-4-gdpr/) (7): “***‘controller’*** *means 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; […].*” For cross-border collaborative projects the controllers of different datasets should be identified. Also, if joint controllership is considered, make sure that all parties understand their obligations, and it is probably good to define the terms for this in an agreement between the parties.

#### What is the legal basis for processing the personal data?

[Article 6](https://gdpr-info.eu/art-6-gdpr/) (1) lists under what conditions the processing is considered lawful. Of these, **Consent** or **Public interest** are relevant when it comes to research. You should determine what legal basis (or bases) you have for processing the personal data in your project.

Traditionally, *consent* has been the basis for processing personal data for research, but under the GDPR there cannot be an imbalance between the processor and the data subject for it to be considered to be freely given. In some countries the use of *consent* as the legal basis for processing by universities for research purposes is therefore not recommended. In those cases, *public interest* should probably be your legal basis. Note that if your legal basis for processing is *consent*, [a number of requirements](https://gdpr-info.eu/issues/consent/) exists for the consent to be considered valid under the GDPR. Consents given before the GDPR might not live up to this.

Also note that even if *public interest* is the legal basis, other laws and research ethics standards might still require you to have consent from the subjects for performing the research.

Please consult with the Data Protection Officer of your organisation on which legal basis to apply to your data.

#### What are the exemptions for the prohibition for processing of special categories of data (such as health and genetic data) under Art. 9 GDPR used?

Processing of certain categories of personal data is not allowed unless there are exemptions in law to allow this. Among these categories (“sensitive data”) are “*‘[...] data revealing racial or ethnic origin, [...] genetic data, [...] data concerning health’*”. Most types of personal data collected in biomedical research will fall under these categories. [Article 9](https://gdpr-info.eu/art-9-gdpr/) (2) lists a number of exemptions that apply, of which *consent* and *scientific research* are most likely to be relevant for research. Please consult with your Data Protection Officer of your organisation.

#### Have data processing agreements been established between the data controller(s) and any data processors?

[Article 4](https://gdpr-info.eu/art-4-gdpr/) (8): “*‘****processor****’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*” Examples of this is if you use a secure computing environment provided by another organisation to do your analysis or to store the data, along with several other scenarios. In the case that you do, there needs to be a legal agreement established between the *controller*(s) and *processor*(s) as defined in [Article 28](https://gdpr-info.eu/art-28-gdpr/) (3): “*Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. […]*” Article 28 also lists the required contents of such an agreement. Your organisation and/or the processor organisation will probably have agreement templates that you can use.

#### Have Data Protection Impact Assessments (DPIA) been performed for the personal data?

Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, a so called **Data Protection Impact Assessment** (DPIA) - [Article 35](https://gdpr-info.eu/art-35-gdpr/). To clarify when this is necessary, the Data Protection Authorities (DPAs) in [Denmark](https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger/), [Finland](https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista), [Norway](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/) and [Sweden](https://www.datainspektionen.se/globalassets/dokument/beslut/list-regarding-data-protection-impact-assessments.pdf) have issued guidance of when an impact assessment is required. Large-scale processing of sensitive data such as genetic or other health related data is listed by all DPAs as requiring DPIAs. The French DPA has made a [PIA tool](https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment) (endorsed by several other DPAs) available that can help in performing these impact assessments. Please also consult your Data Protection Officer of your organisation.

#### What technical and procedural safeguards have been established for processing the data?

To ensure that the personal data that you process in the project is protected at an appropriate level, you should apply technical and procedural safeguards to ensure that the rights of the data subjects are not violated. Examples of such measures include, but are not limited to, pseudonymisation end encryption of data, the use of computing and storage environments with heightened security, and clear and documented procedures for project members to follow.

#### What happens with the data after project completion?

The GDPR states that the processing (including storing) of personal data should stop when the intended purpose of the processing is done. There are, however, exemptions to this e.g. when the processing is done for research purposes. Also, from a research ethics point of view, research data should be kept to make it possible for others to validate published research findings and reuse data for new discoveries. This is also governed by what the data subjects have been informed about regarding how you will treat the data after project completion. The recommendation is to deposit the sensitive data in the appropriate controlled access repositories if such are available, but this requires that the data subjects are informed and have agreed to this.

### Other considerations

There might also exist other national legal or procedural considerations for cross-border research collaborations. Other laws might affect how and if data can or cannot be made available outside the country of origin. The operating procedures of government authorities or other organisations might create obstacles for sharing data across borders. To make sure that it is clear how original and derived data, as well as results, can be used by the parties after the project completion, consider establishing legal agreements that defines this. This can include e.g. reuse of data for other projects or intellectual property rights derived from the research project.