## A response template for Data Management (Part C) and GDPR (Part D) parts of the ethics application at TSB

## Part C: Data Management

Fill in this part completely regardless of the type of research (Category 1 or 2) you are performing. The DMP is obligatory for every research project. For more information check the following webpage: [When and how do I draw up a data management plan? | Tilburg University](https://www.tilburguniversity.edu/intranet/research-support-portal/rdm/datamangementplan). Or contact Jeske de Vet (Data Representative TSB).

**Data storage during research**

The following questions relate to the data collection and data storage period. These are dates when all data are collected and analyzed to conduct the research. **6.1 Where will the data be stored during the data collection and data analyzing period?**

[ ]  O-drive

[ ]  Research drive

[ ]  Surfdrive

[ ]  SharePoint

[ ]  Other, i.e. <insert storage location>

**6.2 Who has access to the raw data during the data collection and data analyzing period?***Please note the names and roles. Note that a minimum of 2 people should have access to the data.*

|  |
| --- |
| TSB default answer: [Name], principal investigator[Name], supervisor/co-researcher |

**6.3 Who has access to the processed data during the data collection and data analyzing period?***Please note the names and roles. Note that a minimum of 2 people should have access to the data.*

|  |
| --- |
| TSB default answer: [Name], principal investigator[Name], supervisor/co-researcherEtc.  |

**Data Archiving period**

Data storage during data archiving. The following questions apply to data archiving. After the research is completed and the data is stored in a secure (digital) facility.

**6.4 Where will the data be archived?**

[x]  DataVerse

[ ]  O-drive

[ ]  Other, i.e. <insert storage location>

**6.5 Who will have access to the raw data during the data archiving period?***Please note the names and roles. Note that a minimum of 2 people should have access to the data.*

|  |
| --- |
| TSB default answer: [Name], principal investigator[Name], supervisor/co-researcher |

**6.6 Who will have access to the processed data during the data archiving period?***Please note the names and roles. Note that a minimum of 2 people should have access to the data.*

|  |
| --- |
| TSB default answer: [Name], principal investigator[Name], supervisor/co-researcher |

**6.7 How long will the data be archived (in years)? And which criteria will you use to decide which data will have to be archived for long-term retention and access? Which (part of the) data will have to be destroyed to ensure privacy protection?**

|  |
| --- |
| TSB default answer: We intend to archive the anonymous data for at least 10 years. We will make anonymous data publicly available via certified data repositories. Personal data (e.g., names, addresses, etc.) will not be shared.  |

**6.8 What documentation and metadata will be provided and what metadata standard will be used (if any)?**

|  |
| --- |
| TSB default answer: We will follow Tilburg University Dataverse guidelines and will provide documentation and metadata following the DDI standard.OrWe will provide documentation and metadata according to the guidelines of the TSB Science Committee.  |

**6.9 Are you allowed to dispose of the data after the research project ends?**

[ ]  Yes

[x]  No, <Because the data needs to be stored for a period of 10 years.>

**6.10 In case of non-digital data storage of the main data of a study**

**What kind of non-digital data will need to be stored during the study (paper surveys, transcripts, photocopies of original documents)? Do these data need special protection to secure privacy and confidentiality? Where will these data be stored? Who will have access to the data?**

|  |
| --- |
|  |

**6.11 Will all or part of the data be made available for reuse after completion of the project according to the FAIR Principles?**

[x]  Yes. Please explain: when and how will the data be made available for re-use? Are there any restrictions for data sharing or any conditions for re-use of the data?

|  |
| --- |
| TSB default answer: All data, materials, and code of our study will be publicly available via the Open Science Framework (OSF) or Dataverse. As a result, the files will be Findable, Accessible, Interoperable, and Reusable. |

[ ]  My data cannot be shared with other researchers for reuse. Please explain why data can’t be shared:

|  |
| --- |
|  |

**6.12 How will ownership of the data and intellectual property rights to the data be managed?**

|  |
| --- |
| TSB default answer: Tilburg University (unless otherwise agreed in an agreement) |

**6.13 Will there be an embargo period for (all or some of) the data?**

[ ]  Yes, namely <embargo time in years>

[ ]  No

**6.14 If applicable, please add a contract defining ownership to the application.**

## Part D: GDPR / Data Processing Register

By filling out this part of the form you are complying with the GDPR which requires personal data be entered in the data processing register of Tilburg University. This includes a pre-DPIA (Data Protection Impact Assessment), which makes it visible whether there are certain risks and whether you are obliged to conduct a DPIA.

Note that some of the fields are “pre-filled” for you as they represent the recommended / standard procedures at TSB.

**7.1 Which personal data are to be collected and processed?**

[ ]  No personal data will be processed. This is the end of the questionnaire, you can skip question 7.2 until 7.8.
[ ]  Yes, namely (multiple answers possible):

**General**[ ] Contact data (for example: name, email address, phone)
[ ] Gender
[ ] Age, birthdate
[ ] Nationality, birth place, birth country
[ ] Student number/employee number
[ ] Experiences (work, education)
[ ] Finances
[ ] Visual materials (pictures, video)
[ ]  IP-address

**Special data**[ ] Racial or ethnic origin[ ] Religious or philosophical beliefs[ ] Political opinions[ ] Health data (e.g. stamina, eating habits, exercise regimen)[ ] Sex life or sexual orientation[ ] Trade union membership[ ] Genetic data[ ] Medical data (e.g. illness, blood values, mental disorder, side effects)
[ ] Biometric data[ ] Criminal records

**Sensitive data**[ ] Copy identification card[ ] R&D meeting[ ] Study results

[ ] **Other**[ ] Namely, Click here to enter text.

**7.2 Will data be anonymized or pseudonymized after collection and if so, who will have access to the identifying file?**

|  |
| --- |
| TSB default answer: After collection, data will be anonymized. All identifiable data will be removed after collection. |

**7.3 Are there any external parties (processors) involved in this study regarding data collection, data storage, archiving and/or other data-related activities? If so, please describe and name them here and state the website(s) of the processor(s) and / or external controller(s).**

A processor is a person or organization to whom or which the responsible party has outsourced the processing of personal data, such as a cloud service. The external party should comply with the GDPR. Some services, such as Surfdrive, comply with these regulations. If an external party is not known to be GDPR compliant, the applicant should ensure that there is a contract to ensure appropriate processing by the external party. This party should take appropriate technical and organizational measures to protect personal data against loss or any form of unlawful processing (e.g. unnecessary collection of data or further processing).

The model processor agreement and procedure is available via [intranet](http://www.tilburguniversity.edu/privacy) or can be requested from one of the [Data Representatives](https://www.tilburguniversity.edu/sites/tiu/files/download/Guideline%20Datapackage%20TSB%202019.pdf).

**Data collection**[ ] Not applicable
[x]  Yes: Qualtrics

**Data storage**[ ] Not applicable
[ ]  Yes: Click here to enter text.

**Data archiving**[ ] Not applicable
[ ]  Yes: Click here to enter text.

**Other data-related activities (e.g. analyses)**[ ] Not applicable
[ ]  Yes:

**Only applicable if there is an external party that requires a processor agreement**

**7.4 Have you agreed upon and centrally archived a processor agreement with the above mentioned processors? Please specify.**

|  |
| --- |
| Tilburg University has a processor agreement with the above mentioned processors.  |

**7.5 What is the legal base for which the processing activity takes place?**

Personal data cannot be processed according to the GDPR unless there is a legal base for processing. This question refers to the legal basis for processing personal data. There are several possibilities, three of which are particularly relevant for research at Tilburg University: (1) consent (participants sign a consent form to process their personal data); (2) Legitimate interest as scientific researcher (“gerechtvaardigd belang”) (for example, this applies to the use of public data from social media where consent is not needed); (3) permission (when an external party provides the applicant with personal data and the external party has obtained consent to use these data).

[x]  (1) Consent (participants sign a consent form to process their personal data);

[ ]  (2) Legitimate interest as scientific researcher (“gerechtvaardigd belang”) (for example, this
 applies to the use of public data from social media where consent is not needed);

[ ] (3) Permission (when an external party provides the applicant with personal data and the
 external party has obtained consent to use these data)

**7.6 Does the applicant receive personal data from or provide personal data to a third party and which of the organizations determines the purpose and means of the processing?**

Thishappens when an applicant receives data from an external party and the external party determines what will happen with the data (e.g., the applicant receives data on which specific analyses have to be conducted). Then it is mandatory to make specific agreements regarding the delineation of the processing. The model processor agreement and procedure is available via [intranet](https://www.tilburguniversity.edu/rdo) or can be requested from one of the [Data Representatives](https://www.tilburguniversity.edu/intranet/research-support/management/storage-archiving-data)

[ ] No

[ ] Yes, data will be sent to:

[ ]  The project group, including Click here to enter text.
 [ ]  Co-researcher from other universities of institutions. Please state their names,
 contact details and countries: Click here to enter text.
[ ]  Other persons responsible for processing the data. Please state their names,
 contact details and countries: Click here to enter text.

[ ] Yes, data access will be provided to:

[ ]  The project group, including Click here to enter text.
 [ ]  Co-researcher from other universities of institutions. Please state their names,
 contact details and countries: Click here to enter text.
[ ]  Other persons responsible for processing the data. Please state their names,
 contact details and countries: Click here to enter text.

**7.7 If applicable, to which third parties (controllers and processors) are the data provided by default? What is the purpose and the basis of this provision?**

Examples are tax authorities, pension funds, health insurers etc. Third parties with an independent processing responsibility are always external and determine their own purpose and resources for the processing. If the data is provided to another controller, then an agreement should be concluded about privacy and security guarantees. This can be done in the agreement that already exists with that other party or in a data exchange agreement for the study for which this clearance is asked.

|  |
| --- |
|  |

**7.8 Data Protection Impact Assessment (DPIA) needed? Tick all that apply. Please note that if two or more boxes are ticked a DPIA is required.**A DPIA is an estimate of the impact of data processing on the data protection of the persons concerned. Such an assessment is required if the intended processing of personal data poses a high privacy risk to the persons concerned, for example if the applicant intends to collect a huge data set or an extremely sensitive data set. Such processing warrants a separate analysis of the risks of the project. Based on this estimate, recommendations can be made to minimize this impact as much as possible or even eliminate it completely.

**Tick all categories[[1]](#footnote-2) that apply to the research. If a DPIA is required, the Data Representative will contact you to schedule this.[[2]](#footnote-3)**

[ ]  **Assessing people on the basis of personal characteristics**: this includes profiling and predicting, particularly on the basis of characteristics such as a person's professional performance, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements. Examples include a bank that determines the creditworthiness of customers (credit scoring), a company that provides DNA tests to consumers to test health risks, and a company that follows visitors to its website and uses this to create profiles of these people.[[3]](#footnote-4)

[ ]  **Automated decisions**: this concerns making decisions with technological means and without human intervention. In order to fall within this category, the decisions should have legal effects or comparable significant effects on the person concerned. Such data processing may, for example, lead to exclusion or discrimination. Data processing with little or no impact on individuals is not covered by this criterion.

[ ]  **Systematic and large-scale monitoring**: this concerns the monitoring of publicly accessible spaces, for example with camera surveillance, but also systematically following data subjects online. Personal data can be collected without those involved knowing who is collecting their data and what happens to it. Additionally, it may be impossible for people to withdraw from this data processing in public places.

[ ]  **Sensitive data**: this concerns special categories of personal data, as laid down in Article 9 of the GDPR: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. Moreover, this category also includes data that are generally regarded as privacy sensitive, such as data about electronic communication, location data and financial data.

[ ]  **Large-scale data processing**: there is no specific definition of this category, but the following criteria should be used to determine whether this is applicable: a. very large datasets concerning many thousands or millions of people; b. the volume of data and/or the range of different data items being processed; c. the duration of the data processing activity; d. the geographical extent of the processing activity.[[4]](#footnote-5)

[ ]  **Combining databases**: Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would make it possible to deduce the personal identities of subjects.

[ ]  **Data concerning vulnerable data subjects**: this applies when there is an unequal balance of power between the data subject and the data controller for example minors, mentally ill persons, asylum seekers, or the elderly, patients, etc.

[ ]  **Use of new technologies**: e.g., combining use of fingerprint and face recognition for improved physical access control, etc. The reason is that this use may involve new ways of collecting and using data, with potentially high privacy risks. The personal and social consequences of using a new technology may even be unknown, a DPIA then helps to understand and remedy the risks.

[ ]  **Data transfer across borders outside the European Union**, taking into consideration, the potential risks of data transfers to such countries.

[ ]  **Blocking of a right, service, or contract**: this concerns data processing that result in data subjects not being able to exercise a right, use a service, or enter into a contract.[[5]](#footnote-6)

**REVIEW FORM RESEARCH PROJECT TSB**

(to be filled in by the reviewer, not the applicant)

Date: Friday, June 02, 2023

**Reviewer comments:**

|  |
| --- |
|  |

**Recommendation:**

[ ]  Accept

[ ]  Revision

[ ]  Rejected

1. The European Working Party 29 (WP29) has indicated nine criteria for which, if there are at least two applicable, a DPIA must be carried out. These criteria are endorsed by the European Data Protection Board and the Dutch Data Protection Agency (“Autoriteit Persoonsgegevens”). Tilburg University has added the criterion about data transfer across borders of the EU due to special regulations that apply in that situation. The criteria are written mostly for large corporations processing personal data and do not take the specifics of scientific research into account. An additional explanation by Tilburg University is given for some of the criteria for scientific research. [↑](#footnote-ref-2)
2. Please note that as a rule of thumb a DPIA is required when two or more categories apply. However, it is possible that a DPIA is required if one or even none of the criteria are applicable. [↑](#footnote-ref-3)
3. At Tilburg University research is conducted in which characteristics of individuals might be used to segment individuals into different groups to explain for example their behavior. This can be seen as profiling. If the processing is done for research purposes and it does not affect the individuals directly, this does not present a high level of privacy risk, which is why in those cases, the criterion **will not** be applicable. However, if the research is conducted as for example contract research and the results directly affect individuals, this criterion **will be** applicable. [↑](#footnote-ref-4)
4. The Dutch Data Protection Agency has determined that for the health care industry 10,000+ individuals make up a large dataset. For other industries, no number has been provided. However, depending on the type of data and the number of data points per individual, a smaller number of individuals might make up a large dataset because the processing of the data will likely present a **high level of privacy risk**. When in doubt, check with your data representative. [↑](#footnote-ref-5)
5. This criterion is applicable for example when covert research is conducted since data subjects are not aware they are being part of scientific research and can therefore not claim their right to information, to object to the processing of their information, etc. [↑](#footnote-ref-6)