Version 20200305

- Ethics Review Board / Data Management / GDPR TSB –

SUBMISSION FORM RESEARCH PROJECT TSB

General guidelines of use

- This submission form must be used for research projects which are going to be executed under supervision of TSB affiliated researchers. Only principal investigators of a project can submit a project for evaluation. At least one of the principal investigators has a PhD and either is employed by Tilburg University or holds an endowed or honorary chair.

- The form consists of four parts. Part A is general information, Part B is the ethical review, Part C is the data management review, and Part D the General Data Protection Regulation (GDPR) review. If your research project has already been ethically reviewed, Part B can be skipped. Please attach the ethical review application and the judgement by the ethics review body to this submission.

- Ethical approval of a research project is valid for the indicated duration of the project or until a change occurs in study population, data collection, or other procedures.

- The researchers and other involved personnel commit themselves to maximize the quality of the research, data analysis, and the reports and to respect specific rules and regulations concerning specific methodologies. The researchers and other involved personnel also guarantee that the study participants may discontinue their participation at all times without any consequences. Below mentioned researchers and other involved personnel commit themselves to treat all participants according to the most recent version of the Helsinki declaration, the Code of Ethics for Research in the Social and Behavioral Sciences involving human participants, and the VSNU Netherlands Code of Conduct for Research Integrity. Moreover, the researchers act in line with the TSB Data Handling and Methods Reporting (DHMR) and the General Data Protection Regulation (GDPR) and the TiU Research Data Management Regulations.

- With this electronic signature the undersigned declares to have described the research project truthfully.

For agreement:

Name: <insert name lead principal investigator>
ANR (employee number): | | | | | | |

Date:

Version 20200305

- Ethics Review Board / Data Management / GDPR TSB –

Part A: General Information

Title research project: <insert title research project>

Principal investigators: <insert title(s) initials last name>

Project duration: <insert proposed start date DD-MM-YYYY> until <insert proposed end date DD-MM-YYYY>

Funding organization (if applicable): <insert names> <grant identifier>

Give a summary of the proposed research project. Make sure you give sufficient information on the data collection procedures (manipulations, stimuli, questionnaires, certainly when they may be ethically sensitive).

1.1 Background

1.2 Research question(s)

1.3 Study design and methodology

1.4 Procedure and materials

1.5 Scientific and societal relevance

Part B: Ethics

2. PARTICIPANTS

2.1 Please check the box that indicates the relevant study population:

☐ Students

☐ General population without complaints

☐ General population with specific "complaints", e.g. stress, pregnancy, medically unexplained complaints

☐ Patients, i.e. <insert the type of patients>

☐ Other, i.e. <insert the type of population>

2.2 Age category of the participants:

☐ Younger than 12 years of age

☐ Older than 11 and younger than 16 years of age

☐ 16 years or older

2.3 Method of recruitment or selection of participants (for example advertisement, conversation with psychologist, voluntary application):

2.4 Organization where the recruitment of participants will take place:

☐ Tilburg University

☐ Other, i.e. <insert name organization(s)> (you have to provide a written agreement that you have permission to execute the study at that/these organization(s))

☐ Not applicable, because <insert reason>

2.5 Reward for participation (multiple answers are possible):

☐ None

☐ Reimbursement of (travel) expenses

☐ Course credit

☐ Financial reward, i.e. <insert amount> €/hours

☐ Other, namely <insert reward>

2.6 Describe in detail the expected burden and/or potential negative consequences for the participants with respect to time, mental, and physical burden.

2.7 Describe measures that have been taken to protect the participant (e.g. insurance, debriefing, etc.):

☐ Not applicable, because <insert reason>

2.8 Are participants subjected to procedures or experiment-related manipulations or tasks? Indicate which ones, and with what purpose.

Examples: interventions, denials (subjects are asked not to smoke, drink alcohol or eat within a certain time frame preceding the study), dietary requests, invasive procedures (e.g. venipuncture to draw blood), medical (e.g. exercise test, fMRI or PET scans) or neuropsychological tests, admissions into hospital/institution, intelligence tests.

3. ADDITIONAL INFORMATION

Please use this space to add information that is important to your project but was not asked about in the form.

4. CHECKLIST INFORMATION TO PARTICIPANT

The information letter requires the following elements:

4.1 What does the study entail?

- Title (Title of the study, if necessary simplified, abbreviated or translated)
- Purpose
- Nature including if the data collection is meant only for training purposes

4.2 What does participating in the study entail?

- Procedures
- Disadvantages/consequences/risks or advantages for the participant

4.3 Information about the participation

- Voluntariness of participation
- Right to decline to participate and withdraw from the research once participation has begun, without any negative consequences, and without providing any explanation
- Right, in principle, to request access to and rectification, erasure, restriction of or object to the processing of the personal data. For more information: www.tilburguniversity.edu/privacy
- Confidentiality protection
- Period of time to which the consent applies (normally the length of the study)
- How the data will be processed
- Period of time that data will be stored and encrypted
- Approval Ethical Review Board (ERB)
- Closing / whom to contact in case of question or additional information requested (name and telephone number/ email address researchers)
- Appendices: Informed Consent

4.4 If applicable

- Applicable insurance guarantees (only if there is additional insurance to the standard insurance)
- Deliberation time
- Procedure for incidental findings
- Re-use of specified data in the current, future or other research
- Incentives for participation (traveling expense, pp hours)

5. CHECKLIST INFORMED CONSENT

- *In case of a mentally incompetent participant, informed consent is obtained from the legal representative(s). It is good practice to also ask the participant where possible.*
- *In case of minors younger than 12 years of age informed consent is obtained from the parent(s) or legal representative(s). It is good practice to also ask the child where possible.*
- *In case of minors older than 11 and younger than 16 years of age informed consent is obtained from both the minor and the parent(s) or legal representative(s).*
- *From 16 years of age, consent is only obtained from the participant. For some types of research it may nevertheless be good practice to inform the parents or legal representatives.*

The informed consent contains the following required elements:

5.1 Mentally competent participants and minors 12-16 year

- Title (Title of the study, if necessary simplified, abbreviated or translated)
- Confirmation that the information is read
- Confirmation that there was room for questions
- Reminder on voluntariness of participation. Right to decline to participate and withdraw from the research once participation has begun, without any negative consequences, and without providing any explanation
- Right, in principle, to request access to and rectification, erasure, restriction of or object to the processing of the personal data. For more information: www.tilburguniversity.edu/privacy
- Permission processing of anonymous/coded data as mentioned in the information letter
- Permission for storing the research data for a period of at least ten years
- Permission participation in the study
- Date, name, signature participant

5.2 Addition/correction for mentally incompetent adults

- Date, name, signature legal representative, relation to participant

5.3 Addition/correction for minors

- Date of birth participant
- Date, name, signature (if possible both) parents/guardians

6. Additional documents that should be added to the application

The following documents should be provided:

☐ Informed consent form

And if applicable:

☐ Participant information letter (precedes participation)

☐ All surveys/questionnaires that will be used

☐ Description of the stimulus materials

☐ Advertisement

☐ Written debriefing

☐ Written consent of organization(s) (except Tilburg University) to recruit participants

Version 20200305

- Ethics Review Board / Data Management / GDPR TSB –

Part C: Data Management

The questions in this section form, together with some questions in section A, the Data Management Plan (DMP) for your research. Please, fill in this part completely regardless of the type of study you are performing. The DMP is obligatory for every research project. For more information check our Tips for writing a Data Management Plan or contact the Research Data Office (all schools) or Reinjet Oostdijk (TSB).

7.1 Data storage

- Storage locations are the digital locations where you store your data: allowed are the TiU network drives (M, O, P), DataverseNL, SharePoint, Surfdrive. You can check here which location is suitable for your type of data. Please note that sensitive data need to be protected.
- Sufficient storage capacity: is the location where you want to store your data large enough to store the data?
- Back up: do you back up the data and if yes, how often?
- Access to raw data. "The raw database is the first database obtained digitally by the staff member. Ideally this should be first digital file created by anyone, but in cases where datasets/secondary datasets from third parties or files e.g. downloaded from data repositories or other types of publicly available databases are used this file may also mean these. Self-collected data means data such as entered questionnaires or data collected by means of online surveys, computers or measuring tools[1]". Please indicate who has access to the raw data and in what time periods? Please mention both the names and the role of the persons who had access, for example: [name], principal investigator, [name], head of department, [name], research assistant, etc.
- Access to processed data, "research ready' data which has been fully calibrated, combined and cleaned/annotated[2]" (university of Leicester). Please indicate who has access to the processed data and in what time periods? Please mention both the names and the role of the persons who had access, for example: [name], principal investigator, [name], head of department, [name], research assistant, etc.
- Storage/archiving period: the period of time the data package is securely stored and saved in the (digital) repository.
- Data collection period: the moments in which all data is gathered to perform the research.
- Data analysis period: the moments in which all data is analyzed to perform the research.
- Data archiving: the period of time after the study has finished and data is stored in a secure (digital) facility.

	Data collection period	Data analysis period	Data archiving
Storage location	<insert location>	<insert location>	<insert location>
Sufficient storage capacity?	<yes or no>	<yes or no>	<yes or no>
Back up	<yes or no & frequency>	<yes or no & frequency>	<yes or no & frequency>
Access to raw data	<role person>	<role person>	<role person>
Access to processed data	<role person>	<role person>	<role person>
Storage/archiving period (years)			<normally ten years, in case of WMO 15 years>

[1] Data Handling Methods Reporting (2017)

7.2 Where will data be preserved long-term (for example a data repository or archive)? Will the repository issue a unique persistent identifier? (e.g., DOI)? Tip: Tilburg University Dataverse is a data repository managed by LIS Research Data Office and is available for all TiU researchers.

7.3 Meta data

Metadata are data about your data and are used to describe your data set/package. They can be descriptive (common fields such as title, author, abstract, keywords which help users to discover online sources through searching and browsing), administrative (preservation, rights management, and technical metadata about formats), or structural (how different components of a set of associated data relate to one another, such as a schema describing relations between tables in a database). A metadata standard is a structured way of describing data. Repositories often use an existing standard. For TiU Dataverse this is the DDI (Data Documentation Initiative) standard.

Please indicate what will be included in your metadata, how it will be documented, and if you use a metadata standard and which one (for guidance see part 7 of the Tips for writing a data management plan).

7.4 Will (part of) the data be made available for reuse after completing the project according to the FAIR Principles? (for guidance see part 6 of the Tips for writing a data management plan).

If yes, please describe in a concrete manner when and how the data will be made available (see part 11 of the Tips for writing a data management plan). Are there possible restrictions to data sharing or embargo

reasons? Are there any conditions for the re-use of the data? If so, which conditions and how will the data be shared? What license will be applied to your research data? For guidance see http://www.dcc.ac.uk/resources/how-guides/license-research-data Tip: data repositories often provide licenses to choose from.

In case the dataset cannot be shared, the reasons for this should be mentioned (e.g. ethical, rules of personal data, intellectual property, commercial, privacy-related, security-related).

7.5 Which criteria will you use to decide which data has to be archived for preservation and long-term access? Which (part of the) data has to be destroyed to ensure privacy protection? For guidance see part 5 of the Tips for writing a data management plan.

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

7.6a 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?

7.6b What kind of data will need to be stored over the required term, of 10 years, for long-term preservation of data? For example: research data of medical studies, processed, anonymized datasets which do not have to be deleted.

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.

8.1 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 8.2 until 8.9.
☐ 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.

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

8.3 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 or can be requested from one of the Data Representatives.

Data collection

☐ Not applicable

☐ Yes: Click here to enter text.

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

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

8.5 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).

☐ (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)

8.6 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?

This happens 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 or can be requested from one of the Data Representatives

☐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.

8.7 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.

8.8 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[3] that apply to the research. If a DPIA is required, the Data Representative will contact you to schedule this.[4]

☐ **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.[5]

☐ **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.[6]

---

[3] 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.

[4] 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.

[5] 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.

[6] 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.

☐ **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.[7]

[7] 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.