

Register of Processings – Manual

Version: 1.0 28 Mei 2018

This manual should help you register your processing. By law the University has to have a register of all personal data processing. This tool provides the DPO-team the necessary overview.

1. Data Controller

Most of the processings for research are carried out under the responsibility of the UT. If you collect and process the personal data yourself or use the results for your own purposes, choose **Yes**.

If another party decides your purposes and tells you how to process the data, choose **No** and enter the **Name of the organization**.

The screenshot shows a form section titled "1 DATA CONTROLLER" with a teal header. Below the header, it says "The Controller is the organization that determines the purpose and means for the processing". A question "1.1.A Is this project being carried out under the responsibility of the UT?" is followed by two radio buttons: "Yes" and "No". Below the radio buttons is a text input field with the label "If not, which organization is the controller?". At the bottom of the section, there is a grey bar with a right-pointing arrow and the text "2 CONTACT".

2. Contact Information

Who should be contacted when the DPO has questions? This is most likely your own information or maybe your supervisors information. The contact person is always an employee of the UT.

3. Processor

If there is a 3rd party involved, handling **on behalf of the UT**, then this 3rd party is a processor. This 3rd party can be a person (often Self-employed without employees) or another organization.

A processor is not a person or organization working with the data, so do not enter all project members here or all people that have access!

Example of processors are hosting providers, external (cloud) tools that are used in your project (for example surveys), etc.

This is often misunderstood, contact your PCP for more information when in doubt. **Most research projects don't have a processor!** Partners in your project (or their personnel) are most likely (co-) controller and not processor.

! If there is **no processor** click the **Remove** button (default number of processors = 1, removing the first (empty) entry sets the number of processors to 0). If you don't remove the processor the tool will warn you about mandatory fields when you save the information. At that moment it is still possible to remove the processor.

The screenshot shows a form titled "3 PROCESSOR". It contains a question: "Is a third party involved in the processing? This concerns every external person or organization who plays a role in processing personal data. This can involve tasks on the content (such as adding or analyzing data to the registration, elaborating interviews or just viewing data) but also technical tasks (such as technical management and hosting of the database on which the registration is stored)." Below this is question 3.1: "How many processors are involved?" with a text input field containing the number "1". A note says: "To enter more than one processor you have to answer question 3 as many times as there are processors." Below this is a section for "PROCESSOR A" with a "Remove" button. Question 3.2.A asks for processor details: "The processor is:" followed by input fields for Name, Address, Postal code, Place, Country, Phone number, and E-mailaddress.

4 Description and lawfulness of processing

The screenshot shows a form titled "4 DESCRIPTION AND LAWFULNESS OF PROCESSING". It contains a question: "What is the name of the processing? If it concerns a processing for research purposes, state the name of the research The processing of personal data is only lawful when there is a legal basis. Check which of the legal bases applies". Below this is question 4.1: "Project X" with a text input field. Question 4.2 asks "Which legal bases apply?" with a list of checkboxes: "Consent of the person concerned" (checked), "Execution of an agreement in which the data subject is a party", "Compliance with a legal obligation", "Protecting the vital interests of the data subject or someone else", "Fulfillment of a task of general interest or public authority", and "Representing the legitimate interests of the controller or a third party". At the bottom, there is a link to "5 PURPOSE OF THE PERSONAL DATA PROCESSING".

For the name of the processing the name of your project is sufficient. Give it a clear name that is easily recognizable and distinct, so 'research for my promotion' is not a useful name.

For research the **legal base** is often "Consent of the person concerned". If asking consent is a problem, contact your Privacy Contact Person.

5 Purpose of the personal data processing

7 PERSONAL DATA AND THE SCOPE OF PROCESSING

5 PURPOSE OF THE PERSONAL DATA PROCESSING

For what purpose are personal data collected and recorded, what is achieved with this? It is important that the relationship can be established between the data collected and the purpose. It is not allowed to collect personal data that are not directly relevant (data minimization). Be specific, for example only 'research' is not enough, describe the goal of the research

5.1

6 WHICH PERSONAL DATA ARE INCLUDED IN THE PROCESSING?

State here what the purpose of the processing is and be concise. **It should be clear from the purpose why you need the specific personal data that you process.** If there is no relation between the purpose and the data you collect, the processing is unlawful. The data collected can only be used for the detailed purpose you state here. So 'Research' is too broad and by law not acceptable as a purpose.

6 Which personal data are included in the processing?

6 WHICH PERSONAL DATA ARE INCLUDED IN THE PROCESSING?

Personal data is any data that can be traced to a natural person, irrespective of whether this is directly possible or indirect, for example by combining different characteristics. Examples of personal data: name, address details, e-mail addresses, location details (including digital), identification numbers, online identification data, characteristics of physical, physiological, genetic, psychological, economic, cultural or social identity.

6.1 About which category of data subjects is data processed?
Example: Students, employees, patients, etc

6.2 Which personal data will be processed?

6.4 What special personal data regarding the mentioned category is processed?

- None
- religion or beliefs
- race or ethnicity
- political alignment
- health
- sex life
- trade union membership
- criminal justice data
- Genetics data
- Biometrics data used to uniquely identify a natural person

6.5 How long are the personal data stored?
The retention period must be related to the purpose of the processing. It is not allowed to keep personal data longer than the purpose for which they were recorded. After that time the data must be wiped or completely anonymised. When personal data under a different law have a mandatory retention period, and this is longer than is appropriate for the purpose of the processing, then this mandatory retention period applies.

6.6 Will the data be erased automatically or manually? (both answers are possible)

- Automatically
- Manually

7 TRANSFER OF PERSONAL DATA

See the text in the application.

7 Transfer of personal data

Here you can enter the parties that use the data under your control. This is the processor (question 3) or any other party (for example the partners in the project) that uses the personal data. Statistical and anonymized data is outside the scope of the GDPR. The transfer of that kind of data should not be mentioned here.

8 Security of personal data

8 SECURITY OF PERSONAL DATA

In what way are the personal details secured? This concerns on the one hand technical measures, such as storage on protected environments and the application of encryption on storage and / or transport. Authorizations are also a form of security. In addition, it concerns procedural agreements such as clear desk and confidentiality declarations and physical access security to rooms (room / cabinet) where, for example, forms are stored.

8.1 Is the personal data secured?
If 'No', go to question 9

No
 Yes

8.2 What measures have been taken to protect personal data against loss, theft, and/or unauthorised use?

Set security policy that has also been implemented
 Physical measures for access security, including organisational control
 Burglar alarm
 Safe for the storage of data files
 Logical access control using specific information (password or PIN)
 Logical access control using a physical element (pass)
 Logical access control using person-specific traits (biometric characteristics)
 Other logical access control
 Automatic logging of access to data, including a verification procedure
 Verification of authorisations granted
 Other security measures

8.3 Is the data processed outside the UT?

No
 Yes, and a written agreement about the protection exists for each processor.
 Yes, and there is NO written agreement about the protection with the processor or one of the processors.

8.4 Who has access to the personal data?

Staff under the direction of the controller
 Staff under the direction of the processor
 Other

8.5 Are the personal data send electronically?

No
 Yes, via local network (UT-net)
 Yes, via a public network (internet)

8.6 Is encryption used?

No
 Yes, the data is encrypted during transmission
 Yes, the data storage is encrypted

9 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OUTSIDE THE EUROPEAN UNION

The security of personal data is very important. You should address this in your **Data Management Plan** in detail (More information: <https://www.utwente.nl/en/lisa/researchsupport/>). To prevent you describing the security in detail twice, only some superficial questions are asked here.

For High-risk projects (with respect to personal data) the PCP can help you with the Data Management Plan.

9 Transfers of personal data to third countries outside the European Union

9 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OUTSIDE THE EUROPEAN UNION

See the website of the Authority for personal data (<https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu>) or contact your Privacy Contact Person.

9.1 Is personal data transferred to one or more countries outside of the European Union during processing?
If 'No', go to question 10

No
 Yes

9.2 Is personal data only transferred to countries outside the European Union that according to the Minister of Justice have an adequate level of protection?

10 PRELIMINARY INVESTIGATION (DPIA)

The GDPR applies to the countries of the European Union. So transfers outside the European Union need extra safeguards (for example Privacy shield regulation for the United States). If you answer yes here you will probably need help from the Privacy Contact Person.

10 Preliminary Investigation (DPIA)

10 PRELIMINARY INVESTIGATION (DPIA)

Is it necessary to carry out a data protection impact assessment prior to starting the processing? This is necessary if there is a processing that probably leads to a high risk for the rights and freedoms of natural persons, especially when a new technology is used. For questions, please contact the Privacy Contact Person.

10.1 Should a DPIA investigation be undertaken?

Yes
 No

STATEMENT OF APPROVAL

There are three criteria under which you will have to do a DPIA (data protection impact assessment).

- A systematic and extended judgement of personal aspects of a living person
- Large-scale processing of special personal data
- Systematic and large-scale monitoring of public space

In practice, this means that a formal privacy impact assessment won't be often needed. When a DPIA is necessary, or when you are in doubt about the necessity, contact the Privacy Contact Person of your faculty.

However, even if you don't have to do a DPIA, we advise you to do an inventory of risks, since this will bring to light which measures you can take to secure the personal data.

Statement of approval

STATEMENT OF APPROVAL

The undersigned declares that the information provided on this form is correct.

Name:

Job name:

Place :

Date of agreement:

Yes, I agree

When you are done, declare that you have provided correct information and click save. Your application will be forwarded to the DPO-team. When it is accepted by them you should receive an automated e-mail.

Thank you for registering your processing. If you have any suggestions or questions, contact your Privacy Contact Person.

See <https://www.utwente.nl/privacy> for more information.