THE PRIVACY FIVE-STEP PLAN

The VU attaches great importance to privacy and the protection of personal data, whether it be our students' data, our employees' data, or the data of others, such as research participants. Hence, the VU takes its legal data protection obligation very seriously. The Director (Business Operations) is ultimately responsible for this, but each of us has a role to play. Together we ensure that we comply with our legal obligation to process personal data in a safe and secure manner.

This document describes the five steps you must take *before* you start a new process, project or research involving the processing of personal data. This step-by-step plan helps you to meet your privacy obligations. It does not answer the question whether a specific form of data processing is allowed or not. This document also focusses exclusively on privacy and therefore does not cover related topics such as ethics, research data management (RDM), procurement law and/or information security. Do you have a question about any of these topics? Then please contact the relevant department.

The five steps:

At each step, if you have any doubts or questions, please contact the Privacy Champion of your faculty or department. They will be happy to help you.

Step 1: Personal data?

Our privacy obligations stem from privacy legislation, including the General Data Protection Regulation (GDPR). The privacy legislation only applies to the processing of personal data. The first question therefore always is: are the data to be processed 'personal data'?

- If yes, then the privacy legislation applies and you proceed to step 2.
- If not, the privacy legislation does not apply. This does not mean that you are free to do whatever you want with the data. The VU may not hold the intellectual property rights to use the data or the data may be (commercially) sensitive in some other way. Therefore, you should always be mindful as to to how you process data, whether it contains personal data or not.

What is personal data?

All information by which a person can be directly or indirectly identified is considered personal data under the privacy legislation. Examples of indirect personal data:

- the 1.90m woman with grey short hair who drives a red convertible;
- the gentleman sitting in the far right-hand seat at the back of the room; or
- a participant number that is or can be linked to a name or e-mail address.

Personal data can be objective or subjective: Caspar thinks Lily is social and engaging. This data reveals something about both Caspar (his opinion) and Lily (that she is sociable and involved, according to Caspar). An example of objective information: Caspar is 1.70 m tall.

What is anonymous data?

Data are anonymous if they cannot be traced back to a person in any way. Anonymous data are not subject to privacy legislation. Examples of anonymous data:

- aggregate data (17% percent of participants have preference X); or
- randomised data (within a group of participants, the data have been randomly swapped so that the participants cannot be traced back to a person). See for example the simulation dataset for universities.

Step 2: Impact analysis (DPIA)

If you want to process personal data in a way that (highly likely) poses great risks for data subjects, you are obliged to carry out a Data Protection Impact Assessment (DPIA). This will enable us to identify the risks and take appropriate measures. If research or other work activities involve the processing of sensitive personal data, it is safe to assume that a DPIA is obligatory. Sensitive personal data includes data that reveals something about someone's health, race, religion, sexual orientation, location, educational performance or financial situation.

Pre-DPIA Questionnaire

To check whether you need to perform a DPIA, we have created a questionnaire: the Pre-DPIA. Filling in the Pre-DPIA is easy, takes about 5 minutes and provides clarity on whether a DPIA is necessary.

DPIA

If the Pre-DPIA shows that a DPIA is necessary, then you must carry out a DPIA. Based on a number of questions, a DPIA tests if what you plan to do is in line with the privacy legislation and how we deal with the risks for those involved.

Support

To carry out a (pre-)DPIA, please contact your Privacy Champion.

Step 3: Agreements

If, in addition to the VU, another party is involved in data processing, in most cases an agreement must be concluded to regulate the mutual rights and obligations. Different situations can be distinguished. The roles played by the VU and the other party in data processing are decisive for which type of agreement is needed.

Data Processing Agreement (DPA)

If the other party processes personal data under the instructions of the VU, the VU must conclude a data processing agreement with that party. This is, for example, the case if an IT application stores data outside the doors of the VU (cloud).

- For VU-wide applications such as Office365, ResearchDrive, SAP or Qualtrics, DPAs have been concluded.

Joint Controllers Agreement

If the VU cooperates with another party and determines together with this party the purpose of the data processing, as well as the way the data will be processed, then the VU must conclude a joint processing agreement with this party. This is, for example, the case when we conduct joint research with other universities.

Data Transfer Agreement

If the VU receives personal data from another party or if the VU provides personal data to another party but they do not otherwise cooperate in data processing, it is advised that the VU enters into a Data Transfer Agreement with the other party.

Support

If you work with another party, please contact your Privacy Champion for information on agreements, templates and, if necessary, referral to the VU privacy legal counsel and/or IXA.

These kind of agreements don't need to be conducted between different faculties or departments within the VU.

Step 4: Privacy statement

Privacy legislation requires us to be transparent about how we handle personal data. To this end, the VU has various general privacy statements and regulations that inform data subjects about how we process and protect personal data. See: https://vu.nl/en/about-vu/more-about/privacy-statement-vrije-universiteit-amsterdam.

Specific privacy statement

The *general* privacy statements of the VU do not focus on any specific processes of data processing. For scientific research or a specific project, it is therefore necessary to draw up a specific statement. Privacy legislation imposes requirements on what must be included in the privacy statement. The VU has a model privacy statement available in Dutch and English that meets these requirements. Please contact your Privacy Champion for this.

Informed consent

It is also possible to include this information in your *informed consent* form. For questions about this, please contact the faculty support or the RDM support desk of the University Library.

Step 5: Registration

The VU is obliged to keep a record of processing activities, in which the processing of personal data is registered. This is also called 'privacy accounting'. As a final step, you should therefore register your new process, project or research in the PrivacyPerfect application. Please contact your Privacy Champion for this.

For the time being, this step does not apply to scientific research. A process is still being developed for this, which will be explained in due course.

Finally

Following this five-step plan will enable you to meet your privacy obligations. Processing personal data is not always permitted and the question of whether the planned processing is permitted is not answered by following this five-step plan.

Below is an overview of the people and departments that can help you in case of questions or concerns:

- Every Faculty and Department has one or more Privacy Champions who answer questions about privacy.
- If you have questions about research data management, please contact the RDM support desk.
- If you have specific legal questions, please contact Institutional and Legal Affairs.
- Did something go wrong and/or do you suspect a data breach? Please contact the IT service desk as soon as possible.
- Do you have a complaint about privacy? Please contact the internal supervisor, the Data Protection Officer.