Teacher

Researcher

Student

Staff

Privacy for staff

Am I still allowed to process personal data?

Under the AVG it is also permitted to process personal data that is necessary to be able to carry out your daily work as an employee. The basic principle is that the processing of personal data in the context of the relationship between employer and employee is permitted.

Information obligation to data subject(s)

If you process personal data, make sure that you inform the person(s) concerned in advance. Many of TU Delft's activities are

listed in the privacy statement on www.tudelft.nl. If your activity is not included, you can make a privacy statement focused on your specific activity. Please mention the following in any case:

- Contact details of the person to contact in case of questions or complaints.
- (Categories of) personal data being processed
- Purpose(s) for which you are going to use the personal data.
- Legal basis (e.g. on the basis of consent of the person(s) concerned.
- If in doubt, consult the privacy team via privacy-tud@tudelft.nl).
- Who has access to the data and/or with whom the data is shared.
- Whether there is a transfer of personal data to countries outside the EU (for example, if a cloud application is running with a US supplier, such as Google or Amazon).
- Retention period of personal data
- The rights of data subjects (e.g. right of access, right of rectification, right to be forgotten, right to object).
- Whether there is automated decision making or profiling.

Storage periods

The AVG does not state for how long you may retain certain personal data. Storage periods are sometimes laid down by law. Think, for example, of the Archives Act or tax legislation. If this is not the case, you as an organisation will have to make agreements about this. The starting point here is: If you no longer need the data for the purpose for which you collected them, delete/anonymise them. This also applies to personal data stored on paper, on the hard disk or in the e-mail box.

CVs may not be kept for more than four weeks after the end of the application procedure. With the consent of the person concerned, you may keep a CV for a maximum of one year.

Archives Act

The Archives Act defines retention periods for many categories of information. The privacy team and the Delft University of Technology archive team work together to gain insight into this. Ask the privacy team for help if you would like to know more about this.

Sharing personal data with study associations

Student associations may only request student data via the University Service ESA. ESA has drawn up guidelines for sharing student data with student associations.

Processing agreement

If you are going to exchange personal data with an external party and TU Delft is responsible for processing the data, a processing agreement must be concluded. TU Delft is responsible for processing when:

- TU Delft has control over the processing and the processor must follow TU Delft's instructions;
- TU Delft determines the purposes and means of data processing;
- TU Delft has instructed a third party to process personal data.
- If an external party is going to exchange personal data with (a department of) TU Delft and the external party is responsible for processing, a processing agreement must be concluded. The external party is responsible for processing when:
  - The external party has control over the processing and TU Delft must follow the instructions of the external party;
  - The external party determines the purposes and means of the data processing;
  - The external party has instructed TU Delft to process personal data. Use the TU Delft template of a processing agreement. Sometimes both TU Delft and the external party are responsible for processing. In such cases, separate

agreements must be made between these joint controllers on how the personal data is handled. An example of this is a partnership between TU Delft and one or more universities in which personal data is exchanged.

Use of images

A photo or video is personal data when people are identifiable. Handle this with care. Do you use the image for reporting purposes (e.g. of an event)? Then you do not need permission. Do you use the image for marketing or promotional purposes? In that case, ask permission beforehand from the person concerned to take photographs and clearly indicate how the person(s) concerned can revoke their permission. Communicate clearly in all cases that photographs are (or can be) taken. If you have any doubts about the purpose for which you use the images, please contact the privacy team.

Use passport/ID

Reading or retrieving an ID, driver's license or passport is only allowed if an organization is legally obliged to do so. TU Delft has this legal obligation, for example, when a new employee is hired (a copy of the passport is requested by HR for the personnel file). Or to apply for a visa for a student. TU Delft also has the obligation to identify students, but a copy of the passport is not required.

Often a proof of identity is required when only a limited set of data is needed, such as a full name or a passport number. Think carefully about what data you really need. If necessary, consult with the privacy team if you can request this information.

Data Protection Impact Assessment (DPIA)

If a processing of personal data involves a 'high risk', a Data Protection Impact Assessment (DPIA) must be carried out. Whether there is a 'high risk' is determined by means of the DPIA pre-screening. The DPIA template and the DPIA pre-screening are

available here.

Privacy by design

Privacy-by-design means that in a new project privacy enhancing measures and data minimization are immediately taken into account. This creates a careful and responsible handling of personal data within the organization.

Privacy by design consists of a number of steps:

- Privacy first: privacy is put first. What are the privacy consequences of the action?
- Think naughtily: put yourself in the shoes of someone who wants to abuse the data and adjust the security accordingly.
- Data minimization: only collect what is actually needed to achieve the goal and no longer.
- Data is not stored longer than necessary, unless there is a legal basis for storing it for a longer period of time (e.g. Archives Act).
- Data will not be processed for purposes other than those established in advance. Research is an exception; secondary use is then permitted.
- Protect data: e.g. through end-to-end encryption.
- Open the black box: the process is and remains transparent to the user.

Data breach

A data breach means that personal data has been lost or an unauthorized person (possibly) has access to the personal data. For example, the loss of a laptop or USB stick, an e-mail sent to the wrong person or authorisations that have not been properly arranged. A data breach is not only IT-related; losing a paper file, for example, is also a data breach. (Suspected) data leaks should always be reported via databreach@tudelft.nl.

Share this page:

Delft University of Technology

Postbus 5
2600 AA Delft
The Netherlands
Tel: +31 (0)15 27 89111
info@tudelft.nl