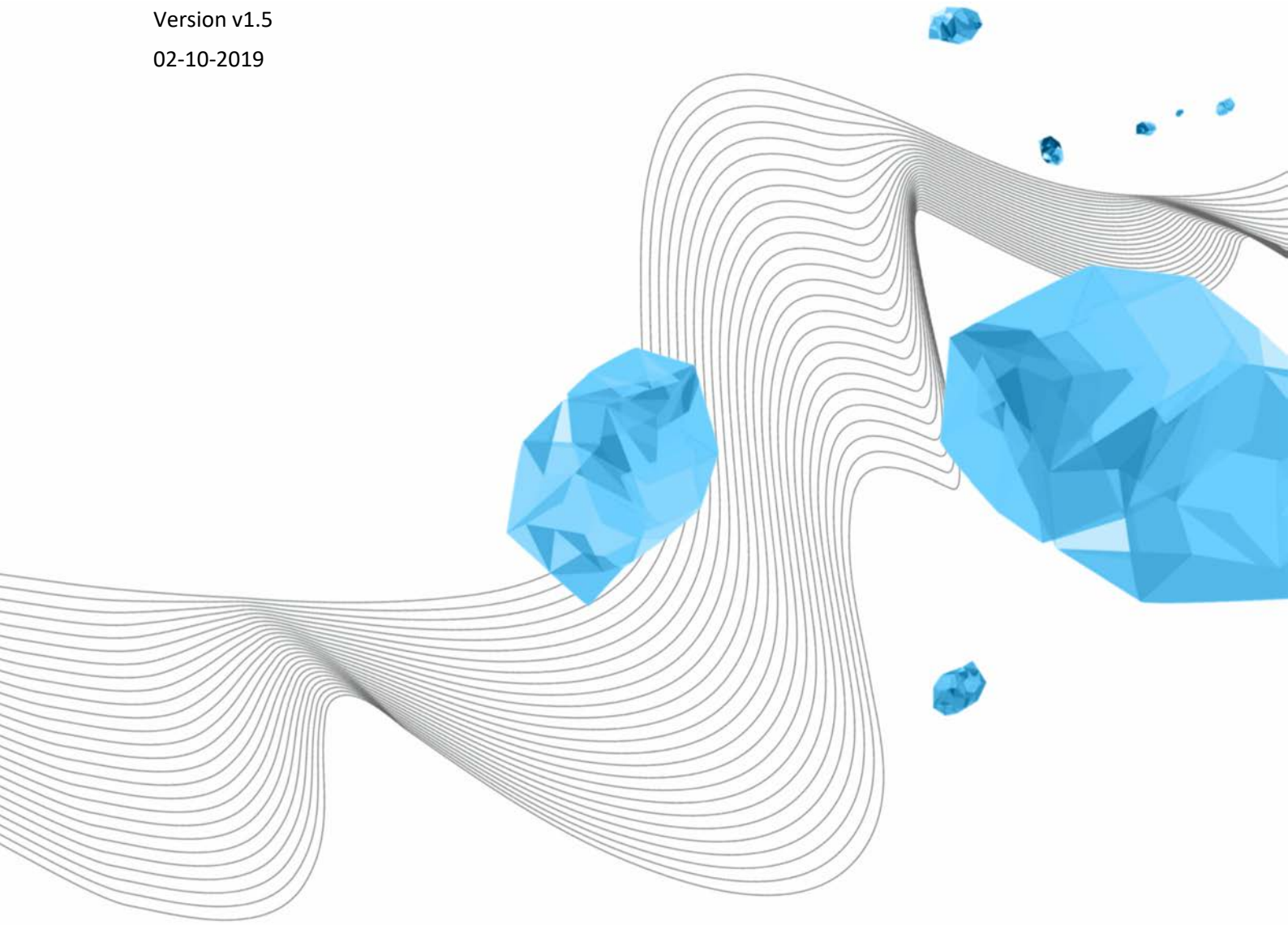
Status: Definitive
Date established by the Board: 14-10-2019
Author: Rianne te Brake/Jan Evers

PRIVACY POLICY UNIVERSITY OF TWENTE

LISA

Version v1.5

02-10-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATION
Library, ICT Services & Archive

TITLE
Privacy Policy University of Twente

KENMERK
UIM/181218/brk

VERSION (STATUS)
v1.5

DATE
02-10-2019

AUTHOR(S)
R. te Brake/J.L. Evers

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	10-10-2016	W. Koolhoven / J.L. Evers	Definitieve eerste versie Vastgesteld in CvB van 17-10-2016
1.1	19-12-2018	R. te Brake	Actualisatie: - Nieuw Model beleid SURF (maart 2018) - Aanvullingen door nieuwe privacywetgeving (AVG) - Kleine correcties
1.2	16-01-2019	R. te Brake	Opmerkingen uit Security + Privacy overleg verwerkt
1.3	12-02-2019	J.L. Evers	Opmerkingen MT LISA verwerkt Bijlage Privacyregels uit het Beleid gehaald; zal als apart document beheerd worden; deze regels geven een praktische vertaling van het Privacybeleid voor verschillende deelgebieden.
1.4	18-06-2019	J.L. Evers	Advies UR dd 5-6-2019 in par. 4.9 verwerkt: begeleider verantwoordelijk voor onderzoek door en voorlichting aan student
1.5	02-10-2019	J.L. Evers	25-09-2019 UR: instemming, onder toezegging van 1. UT-begeleider, 2. cultuurverenigingen toevoegen aan lijst met derden

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.1	19-12-2018	R. te Brake	Leden Security + Privacy overleg
1.2	25-01-2019	J.L. Evers	MT LISA
1.3	12-02-2019	J.L. Evers	02-04-2019 UCB (positief advies) 15-04-2019 CvB (vastgesteld) 24-04-2019 UR (ter informatie)
1.4	18-06-2019	J.L. Evers	01-07-2019 CvB (ter vaststelling) 25-09-2019 UR (ter instemming)
1.5	02-10-2019	J.L. Evers	14-10-2019 CvB (vastgesteld)

TABLE OF CONTENTS

1 INTRODUCTION

In our increasingly digitized society, more and more attention is being devoted to privacy. Staff and students consider privacy to be an increasingly important issue. 'High Tech, Human Touch' means that attention is devoted to privacy in research, education, and operations.

The use of personal data is necessary for the business processes of educational and research institutes. The storage and processing of these personal data must take place with the greatest care, as the abuse of personal data can disadvantage students, staff, and other persons concerned. The Executive Board of the University of Twente is legally responsible for ensuring that personal data is processed in the right way.

By means of the measures described in this policy document, the University of Twente is taking its responsibility for optimizing the quality of the processing and security of personal data and thus satisfying the relevant privacy legislation and regulations.

This policy is based on the "Model beleid verwerking persoonsgegevens" of SURF[1], the organization for cooperation on ICT in Dutch higher education and research. This publication is available under the license "Creative Commons Attribution 4.0 International"[2].

Definitions and abbreviations are included in Appendix 1.

1.1 APPLICABILITY AND OBJECTIVE OF THE PRIVACY POLICY

The privacy policy is important for all staff, students, and other contacts of the University of Twente. This has consequences for the work of all staff and students who work with personal data. The privacy policy relates to the processing of the personal data of all persons concerned within the University of Twente, including in any case all staff members, students, guests, visitors, and external contacts (hiring/outsourcing), as well as to other persons concerned whose personal data the University of Twente processes, for instance experimental subjects participating in scientific research.

The privacy policy does not concern the processing of personal data for personal or internal use, such as personal work notes or a collection of business cards. The privacy policy relates to the fully or partially automated and/or systematic processing of personal data that takes place under the responsibility of the University of Twente as well as the underlying documents (electronic or otherwise). Likewise, the privacy policy applies to the non-automated processing of personal data that have been included in a file or that are intended to be included in that file.

At the University of Twente, the protection of personal data is interpreted broadly. There is an important relationship and partial overlap with the adjoining policy domain of information security, with a focus on the availability, integrity, and confidentiality of data, including personal data. Attention is devoted to these areas of overlap, and harmonization is sought in terms of both planning and content.

The objective of the privacy policy is to optimize the quality of the processing and security of personal data with a focus on finding a good balance between privacy, functionality, and security.

The intention is to respect the private life of the person concerned as much as possible. The details relating to a particular person must be protected against unlawful and unauthorized use and against loss and/or abuse on the basis of the fundamental right to the protection of a person's own personal data. This means that the processing of personal data must satisfy the relevant legislation and regulations, and that personal data are safe at the University of Twente.

The privacy policy provides students, staff, and other concerned persons with insight into how privacy is taken care of at the University of Twente. In addition, this helps with the creation of awareness regarding the importance and necessity of the protection of personal data.

The aims of the privacy policy are:

- To offer a *framework*: to assess current and future processing of personal data against a set best practice or standard and to allocate the tasks, powers, and responsibilities within the organization clearly and consistently.

[1] https://www.surf.nl/files/2019-03/201803-model-beleid-verwerking-persoonsgegevens.pdf
[2] https://creativecommons.org/licenses/by/4.0/deed.en

- To set *standards*: the basis for the security of personal data is ISO 27001.[3] Measures will be taken on the basis of 'best practices' in higher education and on the basis of ISO 27002.[4] The SURF Juridisch Normenkader Cloudservices Hoger Onderwijs [5] is applied as the best practice for cloud services and other outsourcing contracts.
- For the Executive Board to take *responsibility* by setting out the basic principles and the organization of the processing of personal data for the whole of the University of Twente.
- For *decisive* implementation of the privacy policy by making clear choices in measures and applying active control to the execution of the policy measures.
- To be *compliant* with Dutch and European legislation.

In addition to the abovementioned concrete objectives, a more general goal is to create awareness of the importance and the necessity of the protection of personal data, partly in order to avoid risks as a consequence of non-compliance with the relevant legislation and regulations.

[3] In full: NEN-ISO/IEC 27001: Requirements of management systems for information security
[4] In full: NEN-ISO/IEC 27002: Code for information security
[5] SURF juridisch Normenkader (Cloud)services, see https://www.surf.nl/surf-juridisch-normenkader-cloudservices

2 POLICY PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

The general policy principle is that personal data are processed in accordance with the relevant legislation and regulations in a proper and careful manner. In this regard, a good balance needs to be found between the interest of the University of Twente in processing personal data and the interest of the person concerned in making their own choices in a free environment with regard to his/her personal data.

In order to satisfy the above, the following principles apply:

- The processing of personal data is based on one of the legal bases as named in article 6 of the European General Data Protection Regulation (GDPR) (‘legality’). See paragraph 6.1 for list of legal bases.
- Personal data are only processed in a way that is decent and transparent to the person concerned. This means that it must be transparent to the persons concerned to what extent and in what way personal data is processed. Information and communication should be easily accessible and understandable ('decency and transparency').
- Personal data are only processed for specific, explicit and legitimate purposes. These are specific and legitimate purposes, which are laid down and defined before the processing begins. Personal data are not processed in a way that is inconsistent with the purposes for which they were obtained (‘target binding’)
- The processing of personal data takes place in the least drastic manner. This limits the amount and type of data to the data necessary for the specific purpose. For that purpose, the data shall be adequate, relevant and not excessive. (' Minimum data processing ').
- Measures are taken in order to guarantee as far as possible that the personal data to be processed are correct and up to date (‘accuracy’).
- Personal data are kept adequately secure in accordance with the applicable security standards (‘integrity and confidentiality’).
- Personal data are processed for no longer than is necessary for the purposes of the processing. In this regard, the applicable retention and destruction periods are adhered to (‘storage restriction’).

3 LEGISLATION AND REGULATIONS

At the University of Twente, the relevant legislation and regulations are dealt with in the following manner.

3.1 HIGHER EDUCATION AND SCIENTIFIC RESEARCH ACT (WHW)

The University of Twente has a quality assurance system, assuring amongst other things that details in the student administration records are handled carefully, along with the course results. In addition, the integrity code and code of conduct for (non-)scientific personel are also applied and adhered to.

3.2 GENERAL DATA PROTECTION REGULATION

The University of Twente has implemented the legal requirements of the EU General Data Protection Regulation (GDPR) by means of this privacy policy. This concerns, among other things, the lawful and careful processing of personal data and the taking of appropriate technical and organizational measures against the loss and unlawful processing of personal data.

3.3 PUBLIC RECORDS ACT

The University of Twente adheres to the provisions from the Public Records Act, the Public Records Decree regarding the manner in which information recorded in documents (digital or otherwise), information systems, websites, etcetera must be handled.

3.4 TELECOMMUNICATIONS ACT

The University of Twente complies with the regulations regarding, among other things, the use of cookies as described in the Telecommunications Act.

3.5 COPYRIGHT ACT

Amongst other things, the Dutch Copyright Act sets out that the publication of images, photographs, and videos is not permitted if there is a reasonable objection to this on the part of the person concerned (‘portrait right’). The University of Twente applies this regulation.

4 ROLES AND RESPONSIBILITIES WITH REGARD TO THE PROCESSING OF PERSONAL DATA

In order to deal with the processing of personal data in a structured and coordinated manner, a number of roles and responsibilities are allocated to officials within the existing organization.

4.1 OVERLAP WITH INFORMATION SECURITY

The Information Security Officer[6] and the IT Security Manager[7] are closely involved with the implementation of the privacy policy. The careful handling of personal data falls partly under the general rules relating to information security[8].

4.2 THE EXECUTIVE BOARD

The Executive Board (CvB) is the controller and therefore responsible for the lawful and careful processing of personal data within the University of Twente. The Executive Board establishes the policy, the measures, and the procedures around the processing of personal data by means of this privacy policy.

4.3 PORTFOLIO OWNER FOR PRIVACY

The portfolio owner for privacy is the board member with privacy in his/her portfolio. He/she is responsible on behalf of the Executive Board for the security of personal data within the University of Twente.

4.4 DATA PROTECTION OFFICER

The General Data Protection Regulation obliges the University of Twente to appoint an internal supervisor for the processing of personal data. This supervisor is referred to as the Data Protection Officer (DPO). Within the University of Twente, the DPO supervises the application of and compliance with the privacy legislation. The statutory duties and powers of the DPO give this official an independent position within the organization.

The DPO advises and informs the entire organization and the individual units regarding the application of the privacy legislation and will ensure compliance with this. The DPO takes care of the information provision on the processing of personal data to employees, students, and managers. The DPO promotes the privacy awareness of employees and students, for instance by giving information about privacy. An annual privacy report is drawn up each year.

The DPO is the point of contact and expert for those with questions about the protection of personal data. The DPO manages the index of reports of the processing of personal data of the University of Twente and will ensure the execution of the Data Protection Impact Assessment (DPIA).

The DPO is the first point of contact for the supervisory authority (Dutch Data Protection Authority, the AP) and collaborates with him/her.

The Data Protection Officer has the role of process manager of the Privacy Incident process. That means that he/she monitors the university-wide set-up of the process and is responsible for quality assurance.

[6] The role of Information Security Officer is set out in the Information Security Policy.
[7] The role of IT Security Manager is set out in the Information Security Policy.
[8] See the University of Twente Information Security Policy: https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/informatiebeveiligingsbeleid-def.pdf

4.5 SYSTEM OWNER

The system owner[9] is responsible for ensuring that the application and corresponding ICT facilities offer good support for the business process for which they are responsible and that they satisfy the privacy policy. This means that the system owner ensures that the application continues to satisfy the requirements and wishes of the users and the demands of legislation and regulations both now and in the future.

The system owner can be supported in this by the Privacy Contact Person (PCP) and the Data Protection Officer (DPO).

4.6 DIRECTOR

The service department director (service departments) or portfolio holder operations (faculties) is responsible for the implementation of the privacy policy within his or her unit. The director or portfolio holder operations is also responsible for personal data that are entered into an institute system from his/her unit.

The director or portfolio holder operations can be supported in this by the Privacy Contact Person (PCP) and the Data Protection Officer (DPO).

4.7 SUPERVISOR

The creation of awareness and the compliance with the privacy policy are parts of the integrated operational management. Every supervisor has the tasks of:

- ensuring that his/her staff members are aware of the privacy policy and the aspects of the privacy policy that are relevant to them;
- ensuring that the privacy awareness of his/her staff members is adequate;
- ensuring compliance with the privacy policy by the staff members;
- periodically bringing the issue of privacy to the attention of staff members during work discussions.

The supervisor can be supported in this by the Privacy Contact Person (PCP) and the Data Protection Officer (DPO).

4.8 PRIVACY CONTACT PERSON

To support the DPO, there is a Privacy Contact Person (PCP) in each unit service department and faculty. For a university-wide consistent implementation of the privacy policy, the PCP and DPO shall ensure that they are familiar with each other's work. They carry out regular consultations and inform and support each other. The PCP aligns the privacy matters within the unit with the director of portfolio holder operations. Under his/her responsibility, the PCP performs the following tasks on behalf of within the unit:

- ambassadorship in the field of privacy;
- increase privacy awareness;
- safeguarding the attention to privacy in processes;
- advising, training and acting as a center for privacy;
- coordinating information needs;
- support the implementation of a Data Protection Impact Assessment (DPIA);
- support in the recording of data processing operations;
- support the adoption of processors ' agreements;
- advising and supporting data breaches.

[9] See the memorandum ‘Houderschap van een instellingssysteem’, http://www.utwente.nl/nl/sb/beleidsterreinen/universitair-informatiemanagement/it-governance/houderschap-van-een-instellingssysteem.pdf

4.9 RESEARCHER

Every researcher is responsible for the manner in which he or she deals with research data, if appropriate together with a research team leader. The professor or chair of the research group has final responsibility.

The privacy sensitivity and the ethical implications can have consequences for the way in which the research data is handled and the set-up of the research. The principle of proportionality indicates that the processing of the personal data must be proportional to the intended objective or research goal. It is up to the researcher to make this deliberation.

In case research is carried out by a student, the student's UT-supervisor is responsible for the manner in which personal data is handled. The UT-supervisor takes care of a good education and guidance for the student.

4.10 AFFILIATED INSTITUTES

Institutes, foundations, and associations affiliated with the University of Twente are themselves responsible for satisfying the privacy legislation. It is up to the affiliated institute itself to achieve compliance with the (privacy-) legislation. The University of Twente will emphasize the importance of this and ask for insight into how compliance is achieved.

Data processing by affiliated institutes cannot be reported to the Data Protection Officer of the University of Twente. The affiliated institutions are responsible for keeping a register with their personal data processing operations.

For advice, affiliated institutes can appeal to the Data Protection Officer of the University.

5 IMPLEMENTATION OF THE PRIVACY POLICY

The Executive Board is responsible for the processing of the personal data for which they have determined the objective and the means for the processing. They are designated as the *responsible party* in the sense of the General Data Protection Regulation (GDPR). However, the actual processing of personal data is performed in a variety of locations within the university.

The good, efficient, and responsible leadership of an organization is often referred to with the term *governance*. This primarily covers the relationship with the most important interested parties of the University, such as the students, employees, and society. Good governance ensures that all interested parties know their rights and obligations and act accordingly.

5.1 ALLOCATION OF RESPONSIBILITIES

The Executive Board has final responsibility for all data processing of the University of Twente. The responsibilities are assigned in such a manner that every employee has their own responsibility in line with their role.

Privacy is *a line responsibility***.** This means that managers bear the primary responsibility for the careful processing of personal data within their department/unit. This also includes the choice of measures and the performance and maintenance of them. The line responsibility also includes the task of communicating the policy relating to the processing of personal data to all concerned parties within the boundaries of what is reasonable.

Privacy is *everyone's responsibility*. Employees, students, lecturers, and third parties are expected to behave with integrity and to deal with personal data with care. It is for this reason that codes of conduct have been formulated and implemented[10].

5.2 INCORPORATION INTO INSTITUTE GOVERNANCE

In order to allow the cohesion within the organization with regard to data protection to be reflected well and to tailor the initiatives and activities to each other in the field of the processing of personal data within the various elements, it is important to hold structured discussions regarding the topic of privacy at various levels.

At a **strategic level,** guidance is provided on governance and compliance, as well as on objectives, scope, and ambition in the field of privacy (IT Board, Executive Board).

At a **tactical level,** the strategy is translated into plans, standards to be adhered to, and evaluation methods. These plans and instruments provide direction for the operation (University Operations Committee (UCB), I-Beraad).

At an **operational level,** the matters relating to the day-to-day operation are discussed (workplace, Security Managers, Data Protection Officer, Privacy Contact Person, CERT-UT, work discussions).

5.3 AWARENESS AND TRAINING

Policy and measures are not sufficient to exclude risks in the field of processing personal data. It is necessary to continually improve awareness among staff and students relating to privacy and security so that knowledge of risks is increased and good conduct is encouraged. Good practices can be shared with others in the organization, for instance via the Cybersafety website of the University of Twente.

Part of the performance of the privacy policy is the regularly recurring awareness campaigns for employees, students, and third parties. These campaigns can link up with national campaigns in higher education, where possible in coordination with other security campaigns.

Increasing the security and privacy awareness of staff is the responsibility of the managers, who are supported by the Data Protection Officer, the Privacy Contact Persons, the Information Security Officer, and the Security Managers.

[10] See https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/

5.4 CHECKS AND COMPLIANCE

The Data Protection Officer supervises compliance with privacy legislation and the privacy policy, including the allocation of responsibilities, improving awareness, and training personnel. In addition to this, audits make it possible to check the privacy policy and the measures taken in terms of their effectiveness.

Any external checks are performed by independent accountants. This is linked with the annual accountants' audit and is coordinated as far as possible with the normal Planning & Control cycle. Peer reviews of SURFaudit form part of the external checks of the University of Twente.

Should compliance with the protection of data and privacy data fall far short of the required level, the University of Twente can impose a sanction on the responsible employee or student concerned, within the framework of the Collective Labour Agreement and the legal possibilities.

The processing of personal data is a continuous process. Technological and organizational developments within and outside the University of Twente make it necessary to periodically review whether the current course is sufficiently aligned with the policy.

6 LAWFUL AND CAREFUL PROCESSING OF PERSONAL DATA

The University processes personal data in accordance with the principles as elaborated in section 2.1 of this policy. In order to implement these principles, the university shall take the measures set out in this chapter.

6.1 BASIS FOR THE PROCESSING OF PERSONAL DATA

The University of Twente only processes personal data if there is one of the legal grounds as described in article 6 of the GDPR (shown abbreviated):

a. consent of the data subject (the person concerned);
b. necessary for the performance of an agreement with the data subject;
c. necessary to comply with a legal obligation which rests on the controller;
d. necessary to protect the vital interests of the data subject or another natural person;
e. necessary for the fulfilment of a task of general interest or in the exercise of public authority;
f. necessary to protect the legitimate interest of the controller or a third party.

The controller defines the purposes for the processing beforehand. These purposes are formulated concretely and specifically. Each processing is tested to the extent to which the processing of personal data is necessary. The various interests are weighed and the effectiveness, proportionality and subsidiarity are examined. Personal data are not processed in a manner incompatible with the purposes for which they were obtained.

6.2 PRIVACY STATEMENT

The University processes personal data in a way that is fair and transparent to the data subject. This means that the University will provide the data subject with insight into the extent and the way in which their personal data is processed. When collecting the personal data, the University will inform the data subject by means of a privacy statement. The University of Twente has published a general privacy statement on its website. Additional declarations shall be made, if necessary, for specific situations.

Informing data subjects takes place prior to processing, unless this is not reasonably possible. See also section 8.1 of this policy.

6.3 RETENTION PERIODS

Personal data are not retained for longer than necessary for the purposes for which they are collected or used. After the expiry of the retention period,[11] personal data must be put out of reach of the active administrative processes. After the expiry of the retention period, the University of Twente shall destroy the personal data or, if the personal data are intended for historical, statistical, or scientific purposes, the personal data will be saved in an archive.

6.4 APPROPRIATE SECURITY MEASURES

The University is responsible for ensuring an adequate level of security and takes appropriate technical and organizational measures to protect personal data against loss or any form of unlawful processing. These measures also aim to prevent unnecessary or unlawful collection and processing of personal data.

[11] Retention periods can be determined by law, such as in the case of financial details or formal course results, but they can also be determined by the University of Twente, for instance in an agreement between the University of Twente and the persons concerned.

A risk analysis on privacy protection and information security is part of the internal risk management and control system of the university.

6.5 DOCUMENTATION OBLIGATION

The University has taken several measures to demonstrably comply with the legal requirements of the GDPR, including implementation of this privacy policy.

In addition, any fully or partially automated processing of personal data should be reported to the DPO. The DPO assesses the legal validity of the processing and shall ensure adequate documentation of all relevant data.

The University also performs a Data Protection Impact Assessment if necessary. This should at least take place in (research) projects, infrastructural changes or acquisition of new systems that are likely to pose a high risk to the rights and freedoms of natural persons. If the DPIA shows that the processing poses a high risk and the University cannot take measures to mitigate this risk, the University consults the supervisory authority prior to the processing.

6.6 PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

The University uses the principles ' Privacy by Design ' and ' Privacy by Default ' in the implementation of each processing. Privacy by Design concerns the realization of data protection by design, whereby mechanisms are designed to protect the privacy of data subjects as much as possible throughout the life cycle of personal data. Systematic attention is given to, inter alia, the accuracy, confidentiality and integrity of personal data. Privacy by Default is about protecting personal data by means of standard settings of products and services, which are aimed at protecting the privacy of individuals as much as possible.

6.7 CONFIDENTIALITY

At the University of Twente, all personal data are classified as confidential. Everyone should be aware of the confidential nature of personal data and act accordingly.

Even persons who are not already subject to a duty of confidentiality on the basis of their position, profession, or a legal provision are obliged to ensure confidentiality with regard to the personal data of which they have knowledge, except in cases in which any legal provision obliges them to disclose such data or if disclosure of such data is necessitated by their task.

6.8 SPECIAL PERSONAL DATA

In principle, the processing of special personal data is prohibited, unless there is one of the legal exceptions from the GDPR. Possible exceptions include ' explicit consent of the data subject ' and ' weighting general Importance '. In addition, more stringent requirements for the protection of these special personal data apply. Where the basic protection is inadequate, individually tailored additional measures must be taken for each information system.

Special personal data includes the following:

- evidence of racial or ethnic origin;
- political views;
- religious or philosophical beliefs;
- information demonstrating membership of a trade union;
- genetic data for the unique identification of a person;
- biometric data for the unique identification of a person;
- health data;
- data relating to a person's sexual behavior or sexual orientation.

Two types of personal data are not covered by the special personal data category, but their processing and security are subject to strict requirements:

a. processing of personal data relating to criminal convictions and offences may only be done subject to the supervision of the public authorities or when authorised by European or national law;

b. under Dutch law, a national identification number (the BSN or the education number) may only be processed if legally determined.

6.9 TRANSFER OF PERSONAL DATA TO THIRD PARTIES

6.9.1 OUTSOURCING PROCESSING TO A PROCESSOR

If the University of Twente has personal data processed by a *Processor*, the execution of the processing will be set out in a written agreement between the University of Twente, the responsible party, and the processor.

6.9.2 TRANSFER OF PERSONAL DATA WITHIN THE EUROPEAN ECONOMIC AREA (EEA)

The University of Twente only provides personal data to a processor within the EEA, if this processing is based on one of the bases for processing of personal data in article 6 (see paragraph 6.1) of the GDPR and if the processor complies with the legal requirements of the GDPR.
Where the processing contains special personal data, the rules in article 9 of the GDPR also apply.

6.9.3 TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

The University of Twente only provides personal data to third parties located in a country outside the EEA, if one of the following conditions is met:

1. The third country, territory, specific sector in a third country, or the international organisation in question, provides, according to the European Commission, an adequate level of protection.
2. As an adequate level of protection, the University applies:
    - The general list of countries with an appropriate level of protection published by the European Commission[12];
    - The Privacy Shield for companies in the United States, published by the European Commission in cooperation with the US Department of Commerce[13];
3. Transfer takes place on the basis of appropriate safeguards from the GDPR, articles 46 and 47;
4. Transfer takes place on the basis of one of the statutory exceptions in article 49 of the GDPR.

6.9.4 THIRD PARTIES TO WHICH THE UNIVERSITY OF TWENTE TRANSFERS PERSONAL DATA

The University of Twente provides personal data to the following third parties (non-exhaustive list):

- Dutch Education Executive Agency (DUO)
- Government institutions
- Municipalities
- Tax department
- Internship host companies/organizations
- Student residence corporations
- Study societies
- Student associations
- Sports clubs
- Cultural associations

6.10 QUESTIONS AND COMPLAINTS PROCEDURE

6.10.1 NOTIFICATION AND REGISTRATION

Questions or complaints related to (the processing of) personal data can be reported to the Data Protection Officer (dpo@utwente.nl). Of questions or complaints with a (potentially) significant impact, a register is kept.

Anyone, including persons concerned, processors or third parties, can report a question or complaint.

6.10.2 SECURITY VULNERABILITIES

Anyone who perceives a weakness in systems or services of the University of Twente reports it at CERT-UT[14] (cert@utwente.nl). A registry is maintained for all security vulnerability reports.

[12] For this list, see: http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm
[13] For this list, see: www.privacyshield.gov/list.
[14] Computer Emergency Response Team Universiteit Twente

6.10.3 HANDLING

Questions, complaints and security vulnerabilities shall be forwarded to the responsible department or person and shall be dealt with as soon as possible in accordance with the procedures laid down for this purpose. If the personal data of the person (s) or the business processes, the finances or the good name of the university are in danger, the Executive Board is informed in any case.

6.10.4 EVALUATION

It is important to learn from incidents. The registration of incidents and a periodic report on these form part of a professional manner of processing personal data. The reporting on incidents relating to personal data therefore forms a permanent element of the annual privacy report and thus also of the PDCA cycle.

7 DATA BREACH

This chapter describes the policy regarding the reporting, registration and handling of incidents or the presumption of incidents.

7.1 DATA BREACH

A data breach occurs when there is a breach of the security of personal data, which leads to any unauthorized processing thereof. For example, it may include theft of a laptop, a USB stick forgotten in the train, or an email sent to the wrong person. Data breaches should be reported to the supervisor within 72 hours after the controller has taken note of the data breach. In some cases, a data breach should also be reported to the data subject(s).

7.2 REPORTING AND REGISTERING

A data breach at the university may arise within the own organization, but also at a University-enabled processor. Also a person other than an employee, student or processor can identify a data breach. Anyone who perceives a (possibly) data breach or suspects itself to be part of a data breach, will immediately contact the University's reporting point on cert@utwente.nl.

A notification of a (possible) data breach should be made as soon as possible. The following information must be transmitted when reporting a data breach:

- Who has reported?
- What has been reported?
- Where did the notification come from?
- What data does it concern?
- How did the incident occur?
- What systems are involved/touched by the incident?
- When did the incident occur?
- If the report is made by an employee/student of the University: what has been done to resolve the incident/to prevent it in the future?

Records are kept of all incidents and how they were dealt with by CERT-UT.

7.3 HANDLING

In the case of a data breach, this is handled as described in the policy rules “reporting obligation data breaches” of the Dutch Data protection authority[15], so that the reporting of the data breach reaches the right persons and, if necessary, the supervisor and data subjects. The way in which the university handles the reporting and handling of data breaches is described in the procedure for handling data breaches[16].

The underlying security breach is handled by CERT-UT in accordance with the applicable procedures to minimize the likelihood of recurrence and impact.

7.4 EVALUATION

It is important to learn from incidents. The registration of incidents and a periodic report on these form part of a professional manner of processing personal data. The reporting on incidents relating to personal data therefore forms a permanent element of the annual privacy report and thus also of the PDCA cycle.

[15] Beleidsregels meldplicht datalekken Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf.
[16] See www.utwente.nl/nl/cyber-safety/meld-incidenten/procedure-voor-het-afhandelen-van-datalekken.pdf.

8 RIGHTS OF THE DATA SUBJECTS

The GDPR gives data subjects certain rights with which they can control the processing of their personal data. A request may be submitted in writing to the Data Protection Officer (dpo@utwente.nl).

For all the rights of data subjects elaborated in this chapter, the following points apply:

- Notification to data subject
  The University ensures that the information and communication is provided to the data subject in a concise, accessible and comprehensible manner and in clear and simple language. The language is aligned with the target audience.
- Term
  A request from a data subject shall be replied to in writing as soon as possible after submission, but no later than four weeks. In any event, the person concerned shall be informed of the effect given to the request. If the period of four weeks is not reasonably feasible, the data subject shall be informed thereof within this period. In that case, the University will, within two months of the expiry of the first period, follow the request of the person concerned.
- Identity Data subject
  When providing requested information, the University ensures a reliable determination of the identity of the applicant. To this end, the University may request additional information.

  Minors
  A request for the exercise of one of the rights set out in this chapter by a minor, who is underage, has been filed under receiver, or for whom a regime or mentorship has been instituted, is submitted by his legal representative. A response by the university will also be sent to this legal representative.

8.1 RIGHT TO INFORMATION

The data subject has the right to be informed by the university about certain aspects of the processing of his personal data. The university informs the data subject free of charge about the processing of his personal information, both in the situation in which the personal data have been collected directly with the data subject, and when they have been obtained along another route.

a) Obtaining directly from the data subject

The university provides the data subject with at least the following information prior to the collection of the personal data:

- The contact details of the data controller and the DPO.
- The specific purposes of processing for which the personal data are intended and the basis for processing.
- The legitimate interests of the data controller or third party if the processing is based on the 'legitimate interest ' basis.
- Where appropriate, the data controller's intention to transmit the personal information to a third country, which country it is and on what basis the personal data are sent to them.
- The period during which the personal data are stored, or if not possible, the criteria that are used to determine these deadlines.
- The existence of the right to request the controller to inspect, rectify or erase the personal data, restrict the processing concerned, and to object to the processing and the right to data portability.
- The right to submit a complaint with the supervisory authority.
- The recipients or categories of recipients of the personal data.
- If the processing is based on the 'consent' basis, the data subject's right to withdraw that consent at any time.
- Whether the personal data are necessary for the performance of an agreement or to comply with a legal obligation.

- Whether the personal data are used for automated decision-making. The underlying logic as well as the importance and the expected effects of the processing must also be reported to the data subject.

b) Obtaining not directly from the data subject

If the personal data are not collected directly from the data subject itself but along another route, the data subject, in addition to the aforementioned points, shall be provided with the following information

- The categories of personal data.
- The source where the personal data come from.

This information will be provided as soon as possible after obtaining the data, but not later than four weeks, or at the first contact with the person concerned.

8.2 RIGHT OF ACCESS

- Request
  Each data subject has the right to inquire whether his personal data is being processed and, if that is the case, the right to inspect him regarding processed personal data.
- Communication
  If data is processed, the communication from the university contains a complete overview of the following data:
  - A description of the purposes of the processing
  - The categories of data covered by the processing.
  - Categories of recipients
  - Available information about the origin of the data.
  - The period of retention of data or, if that is not possible, the criteria for determining that period.
  - The right of data subject to request the controller to rectify or erase any information, restriction or objection of processing as well as the right to data portability.
  - The right of the data subject to submit a complaint to a supervisory authority.
  - All available information about the source of the data, if the data is not collected from the person concerned.
  - Whether the personal data are used for automated decision-making. The underlying logic as well as the importance and expected effects of the processing must also be reported to the data subject.
  - The appropriate safeguards that have been taken if the data are passed on to a third country.
- Copy
  The person concerned may request a copy of all personal data. This copy should be provided in a common electronic form, unless the request is made on paper or the person concerned explicitly requests a paper copy.
- Cost
  Every first copy can be requested free of charge. For each additional copy, the University may charge an administrative fee to the person concerned.
- Rights and freedoms of others
  The University will take into account the rights and freedoms of others when providing the data.

8.3 RIGHT TO DATA PORTABILITY

- Grounds for Request
  Any person concerned may submit a request to the university to obtain (free of charge) his data in a structured, commonly available and machine-readable form or to transfer it directly to another controller, without being hindered by the university if the following conditions are fulfilled:
  1. The processing by the university rests on the basis of 'consent' or 'execution of an agreement with the data subject';
  2. The processing in question is entirely automated.
- Rights and freedoms of others
  The University will take into account the rights and freedoms of others when providing the data.

- Deletion of data
  If a data subject has exercised his right of data portability in the context of a processing to execute an agreement, the university may not decide to erase the information. However, after the expiry of the retention period, the university must erase the data.
  If the law has been exercised in the context of a processing based on the consent of the data subject, the university may decide to erase the data after exercising the right.

8.4 RIGHT TO RECTIFICATION, COMPLETION, DELETION OR RESTRICTION OF PROCESSING

- Request for rectification, completion, deletion or restriction
  Any data subject may request the University to correct, supplement, delete or restrict the processing of personal data concerning him or her. In the right to restriction, the personal data are temporarily protected and no longer processed by the university. The constraint is clearly indicated in the file.
- Notification
  If it appears that the personal data of the data subject are factually inaccurate, for the purpose or purposes of the processing being incomplete or irrelevant or otherwise processed in breach of a statutory regulation, the data controller (which can be both the functional administrator and the processor) will improve this data, permanently delete it, supplement it or limit it.

  In addition, third parties to whom the data have been provided are informed prior to the rectification, completion, deletion or restriction, unless this is not reasonably possible or in view of the circumstances irrelevant. The applicant may request a declaration from the person to whom the university has made this communication.
- Deadline for implementation
  The data controller shall ensure that a decision to improve, supplement, remove or shield is carried out as soon as possible. The implementation is free of charge for the data subject.

8.5 RIGHT TO OBJECT

- Grounds for objection
  There are two grounds for data subjects to object to a processing:

  1. In connection with his or her personal circumstances, any data subject may object to the processing by the University, if this processing takes place on the basis of:
     a) The fulfilment of a task in the public interest or in the exercise of the authority of the controller, or
     b) The representation of the legitimate interest of the university or of a third party to whom the data are provided.

     For a description of the bases for processing of personal data, see section 6.1.
     The university will in principle discontinue further processing. If the university can demonstrate that its overriding legitimate interests outweigh the interests or fundamental rights and freedoms of the data subject, the processing will continue. If the objection is justified, the university (free of charge) will take measures necessary to stop processing the personal data for the relevant purposes.
  2. When processing personal data with the purpose of ‘direct marketing’, a data subject has the right to object at any time. In case of objection, the University will immediately (free of charge) cease the processing for direct marketing purposes.

8.6 AUTOMATED DECISION-MAKING

- Grounds
  Data subjects have the right not to be subject to a decision based solely on automated processing and to which legal effects are related to him. A ' decision based on automated processing ' means a decision made without any human intervention, for example profiling.

  Only in the following situations can the University take decisions on the basis of automated processing:

1. If the decision is necessary for the conclusion or performance of an agreement with the data subject;
2. If the decision is permitted by a European or national law, provided that this law provides for appropriate measures to protect the rights and freedoms and legitimate interests of the data subject;
3. If the decision is based on the explicit consent of the person concerned. This consent may be revoked at any time.

In all the situations described above, the university will take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject. This includes at least the right to human intervention by the university, the right of the data subject to express his view, as well as the right to challenge the decision. Minors will never be subjected to automated decision-making.

8.7 PROTECTION BY LAW

- General complaints
  If the data subject considers that the statutory provisions concerning the protection of privacy or the provisions of these regulations are not properly enforced against him, he may submit a written complaint to the University.
- Other options to object
  In addition to the general internal complaints procedure, the data subject who considers that the University has committed a violation of the GDPR, has the following possibilities.

  a. Petition procedure at the district court
     If the University has rejected a request as described in section 8.1 to 8.6 of this policy, the person concerned may initiate a petition procedure with the District Court.

     The petition must be submitted to the district court within six weeks of receipt of the University's reply. If the University has not replied to the request of the data subject within the prescribed period, the petition must be submitted within six weeks of the expiry of that period. Submission of the petition does not need to be done by a lawyer.

  b. Objection and appeal
     If the University has rejected a request as described in section 8.1 to 8.6 of this policy and the decision of the University is to be considered as a decision of a governing body within the meaning of article 6 paragraph 4 of the General Administrative Law Act (Awb), the person concerned has the possibility to initiate an objection procedure. This procedure must always be initiated within six weeks of the publication of a decision of the University. Against the decision on objection, an appeal is open to the court.

  c. Enforcement request by supervisory authority
     If the University has rejected a request as described in section 8.1 to 8.6 of this policy, the person concerned has the opportunity to submit a complaint with a supervisory authority or to have an interest organization on his behalf Act.

9 TO CONCLUDE

The privacy policy is evaluated after two years, and a check on the effectiveness of the measures is also included.

For questions or remarks regarding this policy, please contact the Data Protection Officer (dpo@utwente.nl).

APPENDICES

1. DEFINITIONS AND ABBREVIATIONS

Dutch Data Protection Authority: Dutch authority dealing with the protection of personal data. Current name is AP (Autoriteit Persoonsgegevens), old name CBP (College Bescherming Persoonsgegevens).

General Data Protection Regulation: Regulation regarding the processing of personal data and the free movement of such data. Regulation (EU) 2016/679 of the European Parliament and of the Council. The European successor of the Dutch Personal Data Protection Act, effective from May 2018. Referred to as Avg (Algemene Verordening gegevensbescherming).

Data subject: any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected. see Article 4.1 of the GDPR.

Person concerned: an individual and natural person to whom a piece of personal data relates.

Policy: this policy regarding the processing of personal data by the University of Twente.

Personal data: any data relating to an identified or identifiable natural person.

Processing of personal data: every action or every collection of action making up a whole relating to personal data, including in any case the collection, recording, sorting, storing, updating, modifying, retrieval, consulting, use, provision by means of sending, distribution or any other form of making available to others, centralizing, connecting, as well as the protection, exchange, or destruction of data.

Processor: A third party engaged by the University of Twente who, for the benefit of the University of Twente, and on the basis of his written instructions, processes personal data.

Controller: Executive Board of the University of Twente who determines the purpose and means of the processing of personal data.

Third party: Any other person than the person concerned, the person responsible, the processor, or any person who falls under the direct authority of the person responsible or the processor and is authorized to process personal data.

Data breach: Personal data that fall into the hands of third parties who do not have - or are not permitted to have - access to those details.

Data Protection Impact Assessment (DPIA): A review that helps identify privacy risks and provides the handles to reduce these risks to an acceptable level.

Minor: Any person who has not yet reached the age of 16 years.

Privacy by Default: Data protection by using default settings. A data processing in which the default settings of products and services are set up so as to ensure maximum privacy of individuals. This means, among other things, that as few data as possible are requested and processed.

Privacy by Design: Data protection by design. Manage the entire life cycle of personal data, from collection to processing and removal, where mechanisms are designed to take utmost account of the privacy of those involved. Systematic attention is given to comprehensive safeguards regarding accuracy, confidentiality, integrity, physical security and deletion of the personal data.

Profiling: Any form of automated processing of personal data that evaluates certain personal aspects of a natural person on the basis of personal data, in particular with the aim of ensuring professional performance, economic situation, analyze or predict health, personal preferences, interests, reliability, behavior, location or relocation.

EEA: European Economic Area

PDCA: Plan, Do, Check, Act. Improve cycle.

CERT-UT: Computer Emergency Response Team of the University of Twente.

EB: Executive Board

Data Protection Officer (DPO): Official responsible for data protection

Privacy Contact Person (PCP): The privacy contact person of a service department or faculty.

University: The University of Twente

2. EXAMPLES OF DATA BREACHES

Examples of data breaches include:

- a lost/misplaced unencrypted USB stick containing personal data;
- a lost or stolen unencrypted smartphone/laptop/tablet (personal or business) containing personal data or offering access to a University of Twente account containing personal data;
- printed documents containing personal data left unattended at a printer;
- anonymous survey results that can nevertheless be traced to identifiable respondents;
- access to personal data to which you should not have access;
- a hacker breaking into (hacking) a computer containing personal data or offering access to a University of Twente account containing personal data;
- distributing an overview of names, student numbers, and/or course results of students;
- distributing an overview of names, telephone numbers, and/or home addresses of employees;
- unauthorized persons being able to see camera images.

Examples of other privacy incidents are:

- data collection that has not been reported to the Data Protection Officer;
- unsafe working practices that could easily lead to data breaches;
- data collection on the grounds of permission from a person concerned without that permission having actually been requested or recorded.