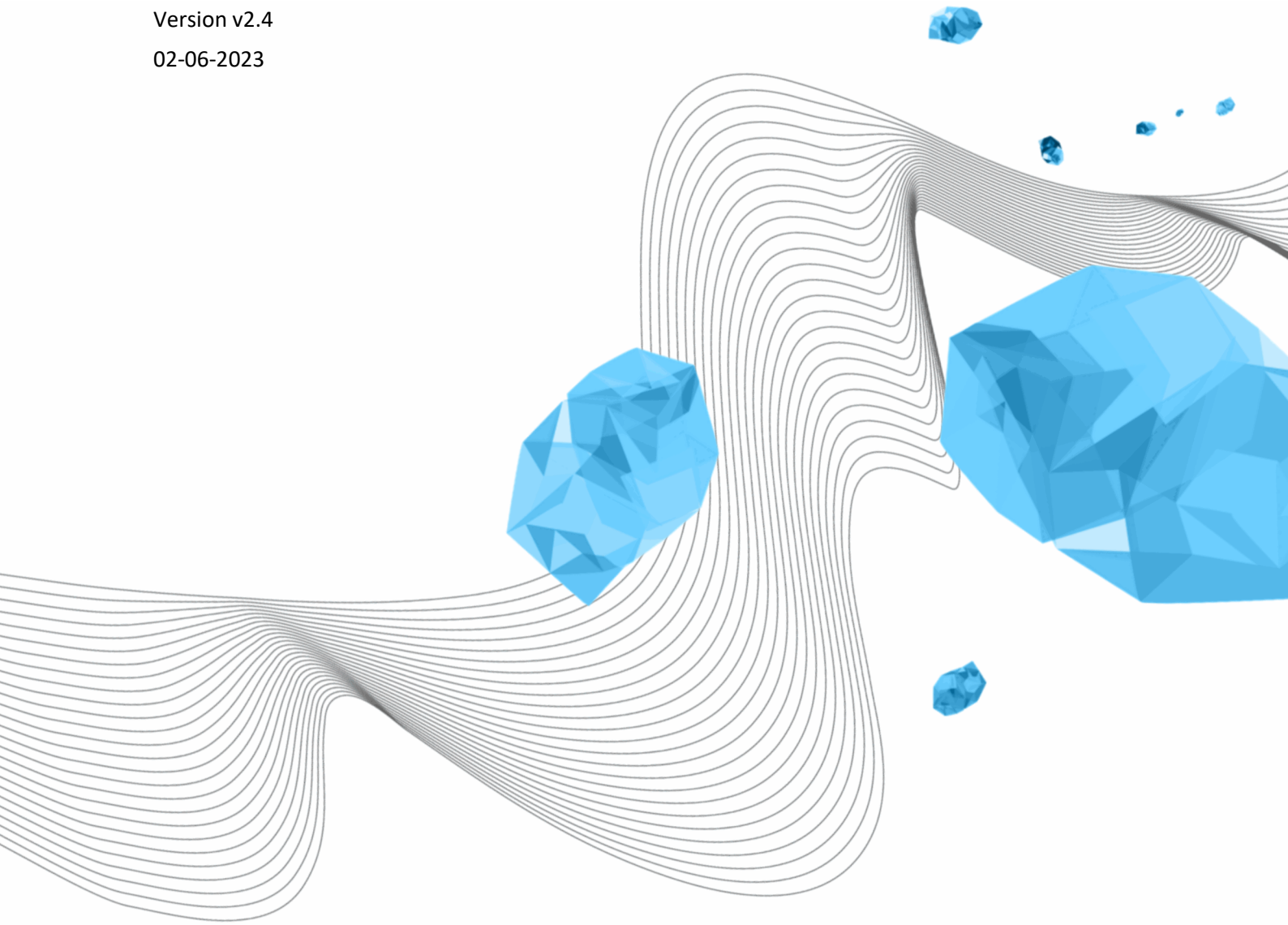
Status: Final
Date established by the Board: 12-06-2023
Author: Rianne te Brake/Jan Evers/Meike van de Ven-Davids/G.B. Meijer

PRIVACY POLICY UNIVERSITY OF TWENTE

LISA

Version v2.4

02-06-2023



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATION
Library, ICT Services & Archive

TITLE
Privacy Policy University of Twente

KENMERK
UIM/181218/brk

VERSION (STATUS)
v2.4

DATE
02-06-2023

AUTHOR(S)
R. te Brake/J.L. Evers/M. van de Ven-Davids/G.B. Meijer

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
1.0	10-10-2016	W. Koolhoven / J.L. Evers	Final first version Established in the Executive Board of 17-10-2016
1.1	19-12-2018	R. te Brake	Actualisation: - New Model policy SURF (March 2018) - Additions following new privacy legisation (GDPR) - Smallcorrections
1.2	16-01-2019	R. te Brake	Comments from Security + Privacy meeting processed
1.3	12-02-2019	J.L. Evers	Comments MT LISA processed Annex Privacyrules deleted from Policy; will be managed as separate document; these rules are a practical translation of the privacy policy for several separate areas.
1.4	18-06-2019	J.L. Evers	Advice University Council of 5-6-2019 in section 4.9processed: supervisor responsible for research by and education to students
1.5	02-10-2019	J.L. Evers	25-09-2019 University Council: approval under condition to add UT supervisors and cultural associations to list of third parties.
2.0	14-10-2022	M. van de Ven-Davids	Actualisation: - New model privacy policy SURF (November 2021) - Align more with the actual situation - Corrections - Align more with the policy principles
2.1	14-11-2022	G.B. Meijer	Review and some adjustments
2.1	06-01-2023	M. van de Ven-Davids	Some adjustments in text and layout
2.2	17-02-2023	M. van de Ven-Davids	Adjustments following comments MT LISA
2.3	03-05-2023	M. van de Ven-Davids	Adjustments following advice UC

[1] https://www.surf.nl/files/2022-02/surf-model-beleid-verwerking-persoonsgegevens-update-2021_0.pdf
[2] https://creativecommons.org/licenses/by/4.0/deed.en

2.4	02-06-2023	M. van de Ven-Davids	Adjustments following advice UC
2.4	12-06-2023	M. van de Ven-Davids	Established by the EB

DISTRIBUTION LIST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
1.1	19-12-2018	R. te Brake	Members Security + Privacy consultation
1.2	25-01-2019	J.L. Evers	MT LISA
1.3	12-02-2019	J.L. Evers	02-04-2019 UCB (positive advice) 15-04-2019 EB (established) 24-04-2019 University Council (for information)
1.4	18-06-2019	J.L. Evers	01-07-2019 EB (to be established) 25-09-2019 University Council (for approval)
1.5	02-10-2019	J.L. Evers	14-10-2019 EB (established)
2.1	06-01-2023	M. van de Ven-Davids	MT LISA
2.2	20-02-2023	M. van de Ven-Davids	MT LISA
2.2	06-03-2023	M. van de Ven-Davids	EB
2.2	30-03-2023	M. van de Ven-Davids	UC
2.3	03-05-2023	M. van de Ven-Davids	EB UC
2.4	02-06-2023	M. van de Ven-Davids	EB UC

TABLE OF CONTENTS

1 INTRODUCTION

In our increasingly digitized society, more and more attention is being devoted to privacy. 'High Tech, Human Touch' is the motto of the University of Twente (UT), and Human Touch implies that attention is devoted to privacy in research, education, and operations. The use of Personal data is necessary for the performance of business processes within the UT. This must take place with the greatest care, as the UT strongly cares about the wellbeing of students, staff and other persons concerned and the abuse of Personal data can disadvantage them.

By means of the measures described in this Policy, the UT 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 an updates version of the Privacy Policy University of Twente of 2 October 2019.

1.1 DEFINITIONS AND ABBREVIATIONS[3]

Anonymising: a method whereby Personal data are Processed in such a way that they can no longer identify a person, not even if the data are combined with other data. This operation is irreversible.

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

Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal data; where the purposes and means of such Processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law. In this Policy the Controller is the EB.

Data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal data transmitted, stored or otherwise Processed.

Data subject: an identified or identifiable natural person to whom Personal data relates.

DPA (Dutch Data Protection Authority): Dutch authority supervising the protection of Personal data; the AP (Autoriteit Persoonsgegevens).

DPIA (Data Protection Impact Assessment): An assessment to help analyse, identify and minimise data protection risks of a project or plan.

DPO (Data Protection Officer): The person appointed by the UT with the primary role to ensure that the UT Processes Personal data in compliance with the applicable data protection rules. The DPO is registered with the DPA and has a DPO-number. The DPO has an independent position at the UT.

DTIA (Data Transfer Impact Assessment): Based on a DTIA, the UT conducts a prior investigation into the privacy risks associated with a transfer of Personal data to a country outside the EEA. The intention is to identify the risks and take additional measures to eliminate them or reduce them as much as possible.

EB: Executive Board

EEA: European Economic Area

GDPR: General Data Protection Regulation. Referred to in Dutch as AVG (Algemene Verordening Gegevensbescherming)[4].

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

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

Policy: this privacy policy

Privacy by default: Data protection by using default settings. The default settings of products and services are set up so as to ensure a maximum level of protection of privacy of individuals. This means, among other things, that as few data as possible are requested and Processed.

[3] Some definitions have been abbreviated for readability. For full definitions see GDPR.
[4] The GDPR entered into force on May 25, 2016 and is effective from May 25, 2018.

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.

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

Processing: Any operation or set of operations which is performed on Personal data or on sets of Personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: A natural or legal person, public authority, agency or other body which Process Personal data on behalf of the UT.

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, analyse or predict health, personal preferences, interests, reliability, behaviour, location or relocation.

Special categories of personal data: Personal data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data natural person's sex life or sexual orientation as referred to in Article 9 GDPR.

Third party: A natural or legal person, public authority, agency or body other than the Data subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to Process Personal data.

UCB: University Committee Management

UT: The University of Twente

1.2 SCOPE AND PURPOSE OF THE PRIVACY POLICY

1.2.1 SCOPE OF THE PRIVACY POLICY

The Policy is important for all staff, students, and other contacts of the UT. This has consequences for the work of all staff and students who work with Personal data. The Policy relates to the Processing of the Personal data of all Data subjects within the UT, 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 UT Processes, for instance experimental subjects participating in scientific research[5].

The 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 Policy relates to the fully or partially automated and/or systematic Processing of Personal data that takes place under the responsibility of the UT as well as the underlying documents (electronic or otherwise). Likewise, the 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.

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 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 Data subjects as much as possible. The details relating to a Data subject 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.

[5] The document 'Appropriate use of personal data in scientific research according to the GDPR' (see https://www.utwente.nl/en/cyber-safety/privacy/guideline-for-research/) specifically handles Processing Personal Data in scientific research.

This means that the Processing of Personal data must satisfy the relevant legislation and regulations, and that Personal data are safe at the UT.

1.2.2 PURPOSE OF THE PRIVACY POLICY

The Policy provides students, staff, and other concerned persons with insight into how the UT protects Personal data. In addition, this helps with the creation of awareness regarding the importance and necessity of the protection of Personal data.

The purposes of the Policy are:

- To offer a *framework*: to assess current and future Processing operations of Personal data against a set best practice or standard and to allocate the tasks, powers, and responsibilities within the organisation clearly and consistently.
- To set *standards*: determine how the UT handles Personal data.
- The SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[6] is applied as the best practice for cloud services and other outsourcing contracts.
- For the EB to take *responsibility* by setting out the basic principles and the organisation of the Processing of Personal data for the UT.
- For *decisive* implementation of the 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.

[6] 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 UT 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:

1. Responsibility:
    - A responsible party has been appointed (internally) for each Processing operation.
    - The Controller enters into agreements with Processors and third parties about the safe and careful Processing of Personal data.
2. Legitimate purpose and legal basis:
    - The purpose of Processing must be sufficiently specific and clearly described prior to Processing.
    - A Processing operation is based on one of the legal bases as mentioned in Article 6 of the GDPR and in paragraph 6.2 of this Policy.
3. Ethically sound
    - Ethical aspects are also taken into account when assessing the Processing of Personal data (it may be allowed, but do we also want this?).
4. Data minimisaton
    - No more Personal data is collected than necessary for the purpose of Processing. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.
    - Processing Personal data takes place in the least intrusive manner and must be in reasonable proportion to the intended purpose (subsidiarity and proportionality).
5. Purpose limitation
    - Personal data will not be further Processed in a manner that is incompatible with the purpose for which the Personal data is collected.
6. Retention and destruction
    - Personal data are provided with a retention period.
    - Personal data will be destroyed or Anonymised when it is no longer necessary to keep them for the purposes of Processing.
7. Accuracy
    - Measures are taken to guarantee as much as possible that the Personal data to be Processed are accurate and up-to-date.
8. Transparency and information
    - It is clear to Data subjects to what extent and in what way Personal data are Processed. Information and communication about this must be easily accessible and understandable, for example by means of a privacy statement.
9. Sharing of Personal data
    - Personal data will only be shared with other parties if this can be based on a legal basis.
    - In case Personal data will be shared with other parties, proper agreements must be in place.

10. Security
    - Personal data are secured by taking appropriate technica land organisational measures (risk-based).
    - Access to Personal data is granted on a need-to-know basis.
    - Systems are designed and set up according tot he principles of Privacy by design and Privacy by default.
11. Rights of Data subjects
    - Every Data subject has the right of access and rectification, erasure and restriction of his/her Personal data, as well as the right to object.
    - If a Processing operation is based on the legal basis ‘consent’, consent must be requested prior to Processing.
    - Consent can be withdrawn just as easily as it has been given.
12. Accountability
    - The UT can demonstrate that she complies with the GDPR.

3 LEGISLATION AND REGULATIONS

At the UT, the relevant legislation and regulations are dealt with in the following manner.

3.1 HIGHER EDUCATION AND SCIENTIFIC RESEARCH ACT (WHW)

The UT 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 AND IMPLEMENTATION ACT GDPR

The UT has implemented the legal requirements of the GDPR and Implementation Act GDPR by means of this 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 LABOR REGULATIONS AND COLLECTIVE EMPLOYMENT AGREEMENT

The UT is responsible for being a good employer, in which (among other things) the careful handling of Personal data in the personnel administration is guaranteed. In addition, Personal data is shared with, for example, the UWV, the Tax and Customs Administration and the company doctor.

3.4 PUBLIC RECORDS ACT

The UT 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.

3.5 TELECOMMUNICATIONS ACT

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

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[7] and the IT Security Manager[8] are closely involved with the implementation of the Policy. The careful handling of Personal data falls partly under the general rules relating to information security[9].

4.2 THE EXECUTIVE BOARD

The EB is the Controller and therefore responsible for the lawful and careful Processing of Personal data within the UT. The EB establishes the policy, the measures, and the procedures around the Processing of Personal data by means of this 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 EB for the security of Personal data within the UT.

4.4 DATA PROTECTION OFFICER

The GDPR obliges the UT to appoint an internal supervisor for the Processing of Personal data. This supervisor is referred to as the DPO. The DPO must be involved in a timely manner by the UT in all matters involving Personal data. Within the UT, the DPO supervises and monitors the application of and compliance with privacy legislation. The statutory duties and powers of the DPO give the DPO an independent position within the organization. The UT registers the DPO with the DPA.

The duties of the DPO are:

- Informing and advising all parties involved about their obligations under the GDPR.
- Monitoring compliance with the GDPR and other relevant privacy legislation.
- Monitoring compliance with this Policy.
- Monitoring allocation of responsibilities, awareness and training of relevant personnel and audits.
- Adivsing on and supervising the execution of DPIAs.
- Handling complaints and/or questions that are addressed directly to the DPO.
- Cooperating with the DPA.
- Acting as the first point of contact for the DPA.

4.5 SYSTEM OWNER

The system owner is responsible for ensuring that the application and corresponding ICT facilities are in line with the Policy. This means that the system owner ensures that the application continues to

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

satisfy the requirements and wishes of the users and the demands of legislation and regulations both now and in the future.

The system owner has the following duties:

- Registration of Processing operations in the register of processing activities.
- Making written agreements about sharing Personal data, for example by means of a processing agreement[10].
- Identifying risks in Processing operations (DPIA and/or DTIA)[11].
- Carrying out the measures necessary to mitigate the risks.

The system owner can be supported in this by the PCP of the relevant unit and the DPO.

4.6 DIRECTOR

The service department director (service departments) or portfolio holder operations (faculties) is responsible for the implementation of the 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 PCP and the DPO.

4.7 SUPERVISOR

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

- ensuring that his/her staff members are aware of the Policy and the aspects of the Policy that are relevant to them;
- ensuring that the privacy awareness of his/her staff members is adequate;
- ensuring compliance with the 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 PCP and the DPO.

4.8 PRIVACY CONTACT PERSON

To support the DPO, there is a PCP in each unit service department and faculty. For a university-wide consistent implementation of the 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 DPIA and/or DTIA;
- support in the recording of data Processing operations;
- support the adoption of Processors ' agreements;
- advising and supporting Data breaches.

[10] The UT uses models of, amongst others, data processing agreements. Signed agreements must also be included in the register of processing activities.
[11] The UT uses models of DPIAs and DTIAs. Performed DPIAs and DTIAs must also be included in the register of processing activities.

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 UT are themselves responsible for satisfying the privacy legislation. It is up to the affiliated institute itself to achieve compliance with the (privacy-) legislation. The UT 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 DPO of the UT. The affiliated institutions are responsible for keeping a register with their Personal data Processing operations.

For advice, affiliated institutes can appeal to the DPO of the UT.

4.11 ALLOCATION OF RESPONSIBILITIES

Carefully Processing Personal data 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 and alignment with the DPO regarding the 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.

Carefully Processing Personal data 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[12].

Everyone involved in the UT, including employees and students, is expected to report a Data breach or suspicion thereof to CERT-UT (cert@utwente.nl). A Data breach procedure is in place, in which the DPO plays an advisory role.

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

5 IMPLEMENTATION OF THE PRIVACY POLICY

5.1 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, EB).

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, DPO, PCP, CERT-UT, work discussions).

The DPO advises and supervises within all levels.

5.2 AWARENESS AND TRAINING

Policy and technical and organisational 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 safe and responsible conduct is encouraged. Good practices can be shared with others in the organization, for instance via the Cybersafety website of the UT.

Part of the performance of the 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 DPO, the PCPs, the Information Security Officer, and the Security Managers.

5.3 CHECKS AND COMPLIANCE

The DPO supervises compliance with privacy legislation and the Policy. In addition to this, audits make it possible to check the 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 UT.

Should compliance with the protection of data and privacy data fall far short of the required level, the UT 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 UT 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 UT Processes Personal data in accordance with the principles as elaborated in section 2.1 of this Policy. In order to implement these principles, the UT shall take the measures set out in this chapter.

6.1 RESPONSIBILITY

A responsible person is designated for each data Processing operation. Usually, this is the system owner (see 4.5). The responsible party ensures that Processing complies with the principles of this Policy and, if necessary, has a DPIA or DTIA carried out. By means of a DPIA, risks related to the Processing of Personal data are identified and measures to reduce these risks are applied by the system or process owner. On the basis of a DTIA, an organization conducts prior research into the privacy risks involved in the transfer of Personal data to a country outside the EEA. The intention is to identify the risks and take additional measures to eliminate them or reduce them as much as possible.

In partnerships and in the case of outsourcing, it is not always immediately clear who should be regarded as the Controller. Clarity about this when making contract agreements is necessary. The Controller is the person who determines the purpose and means of the Processing. The DPO can support and advise on the question of who should be regarded as the Controller.

The Controller enters into agreements with Processors and any third parties about the safe and careful Processing of Personal data. The model agreements of the UT are used to make agreements with other parties about the Processing and exchange of Personal data. The PCPs and the DPO can advise on this.

6.2 LEGITIMATE PURPOSE AND LEGAL BASIS

The UT only Processes Personal data if there is a legitimate purpose for doing so. The purpose of Processing is sufficiently specific and clearly described prior to the Processing. This is, among other things, recorded in the Processing register. The PCPs and DPO can assist with the registration in the Processing register.

The UT only Processes Personal data if one of the legal grounds as described in Article 6 of the GDPR applies:

1. consent of the Data subject;
2. necessary for the performance of an agreement with the Data subject;
3. necessary to comply with a legal obligation to which the Controller is subject;
4. necessary to protect the vital interests of the Data subject or another natural person;
5. necessary for the performance of a task of public interest or in the exercise of public authority;
6. necessary for the protection of the legitimate interest of the Controller or a Third party.

When using the “consent” basis, the Data subject is informed prior to that consent is given about the purpose of the data Processing in accordance with what is stated in 6.9.1 under the right to information. The UT can demonstrate:

i. how this consent was requested;
ii. that this consent has been given specifically for the purpose described; and
iii. that this consent has been unambiguously granted.

The UT ensures that withdrawing consent is just as easy as giving it. The UT informs the Data subject in advance that the withdrawal of consent does not affect the lawfulness of the Processing until the moment of withdrawal. Withdrawal of consent does not have retroactive effect.

The UT takes into account that consent must be given freely without direct or indirect pressure. Since there is a power relationship between the UT on the one hand and students or employees on the other, it will have to be well motivated why consent can be freely given in the specific case.

Special categories of personal data

In principle, the Processing of Special categories of personal data is prohibited, unless a legal exception applies (e.g. when the Data subject has given explicit consent; exceptions also apply for scientific research). In addition, stricter requirements apply to the security of Special categories of personal data. Where the basic protection is not sufficient, individually tailored additional measures must be taken for each information system.

6.3 ETHICALLY RESPONSIBLE

Ethical aspects are also taken into account when assessing the Processing of Personal data (perhaps it is allowed, but do we also want this?). These aspects are taken into account in particular in Processing operations that are intended to be used for Profiling or that, by their nature, require it, for example because new technologies are used.

Ethical aspects also play a role in human-related research. If the research is also subject to the Social Support Act (WMO)[13], it must be reviewed by a recognized medical ethics committee.

6.4 DATA MINIMISATION

No more data is collected than necessary for the purpose that the UT wants to achieve by Processing that data. Personal data must be adequate, relevant and not excessive.

Processing of Personal data takes place in the least intrusive manner and must be in reasonable proportion to the intended purpose (principle of subsidiarity and proportionality). If the purpose can also be achieved in a way that infringes less on the privacy of the Data subject, then this way is chosen. (Think, for example, of asking for a date of birth vs asking for an age category or collecting data Anonymously.)

The UT applies Privacy by default and Privacy by design when new systems or processes are taken into use.

Privacy by design refers to the realisation of data protection by design, where mechanisms are designed to protect the privacy of Data subjects as much as possible throughout the life cycle of Personal data. In doing so, attention is systematically paid to, among other things, the accuracy, confidentiality and integrity of Personal data.

Privacy by default concerns the protection of Personal data by means of standard settings of products and services, which are aimed as far as possible at protecting the privacy of Data subjects.

6.5 PURPOSE LIMITATION

Personal data collected for a specific purpose may only be further Processed for other purposes if these other purposes are compatible with the initial purpose.

If the UT deems further Processing desirable, the following must be checked to determine whether the further Processing is compatible:

- The relationship between the intended new purpose and the initial purpose of Processing. The closer the two purposes are, the more likely it will be that the further Processing of Personal data will be compatible with the initial purpose.

[13] https://english.ccmo.nl/investigators/legal-framework-for-medical-scientific-research/your-research-is-it-subject-to-the-wmo-or-not

- The context in which the Personal data was collected. This takes into account to a large extent the reasonable expectation that the Data subject may have regarding the further Processing of his Personal data for this new purpose.
- The nature of the Personal data. For example, sensitive Personal data deserve a higher level of protection and they are less likely to be used for other purposes.
- The possible consequences of further Processing for Data subjects.
- The existence of appropriate safeguards, such as encryption or the use of pseudonymised Personal data.

The further Processing of Personal data for scientific and historical research, for statistical purposes and for archiving purposes in the public interest are considered compatible by the GDPR, provided that sufficient appropriate technical and organizational measures have been applied, such as the pseudonymisation of Personal data.

If the UT wishes to Process Personal data for a purpose that is incompatible with the initial purpose, this is only possible if the Data subject has given consent for this or in the event of a specific legal obligation to provide certain Personal data to a government body. In such a case, this is considered a new Processing operation and the lawfulness, carefulness and necessity of this must be assessed again.

6.6 RETENTION AND DESCTRUCTION OF PERSONAL DATA

Personal data may not be kept longer than necessary for the purposes for which the data are collected or used. The UT will destroy or Anonymise the Personal data after the retention period has expired or, if the Personal data are intended for historical, statistical or scientific purposes, store it in an archive and take appropriate technical and organisational measures, such as pseudonymisation.

6.7 CORRECTNESS

Measures are taken to guarantee as much as possible that the Personal data to be Processed are correct and up-to-date. These measures may differ per process/system. Incorrect or outdated Personal data will be corrected or deleted. The UT is active in keeping Personal data correct and up to date. Processes and systems are designed and set up in such a way that the correctness of Personal data is enforced and verifiable as much as possible.

6.8 TRANSPARENCY AND INFORMATION

The UT Processes Personal data in a manner that is fair and transparent with regard to the Data subject. This means that the UT will make it clear to the Data subject, among other things, to what extent and in what way his Personal data is Processed, for example by means of a privacy statement or information letter. Informing Data subjects takes place prior to Processing, unless this is not reasonably possible.

6.8.1 RIGHT TO INFORMATION

The Data subject has the right to be informed by the UT about certain aspects of the Processing of his Personal data, for example by means of a privacy statement. The UT informs the Data subject about the Processing of his Personal data, both in the situation in which the Personal data has been collected directly from the Data subject and when they have been obtained via a different route. The UT can demonstrate that the information has been provided.

6.9.1.1 OBTAINED DIRECTLY FROM THE DATA SUBJECT

Prior to the collection of the Personal data, the UT will provide the Data subject with at least the following information if the Personal data is collected directly from the Data subject:

- The identity and contact details of the Controller and the DPO;
- The purposes and legal basis of the Processing;
    - When the Processing is based on the basis of 'legitimate interest': the legitimate interests of the Controller or Third party;
- The (categories of) recipients of the Personal data;
- Where applicable, the intention of the Controller to transfer the Personal data to a country outside the EEA, which country this is and on what legal basis;
- The retention period of the Personal data or the criteria for determining this period;
- The rights of Data subjects;
- If the Processing is based on the basis of 'consent', the right of the Data subject to withdraw that consent at any time;
- The right to lodge a complaint with the DPA;
- Whether and why the Data subject is obliged to provide the Personal data and what the consequences are if the Personal data are not provided;
- Whether automated decision-making (including Profiling) is used.

6.9.1.2 NOT OBTAINED DIRECTLY FROM THE DATA SUBJECT

If the Personal data was not collected directly from the Data subject himself, but via another route, the Data subject will be provided with the following information in addition to the points mentioned above:

- The categories of Personal data;
- The source from which the Personal data originates.

This information will be provided as soon as possible, but not later than one month, after obtaining the Personal data, or upon the first contact with the Data subject.

6.9 SHARING PERSONAL DATA

6.9.1 PROCESSING BY A PROCESSOR

If the UT has Personal data Processed by a Processor, the execution of Processing is regulated in a written data processing agreement between the UT, the Controller, and the Processor. A data processing agreement is agreed prior to the start of the relevant Processing operation.

6.9.2 PROCESSING BY OR JOINTLY WITH ANOTHER CONTROLLER

If the UT determines the purposes and means for the Processing of Personal data together with one or more parties, then these parties have a joint processing responsibility. The parties will enter into an agreement regarding the careful and safe Processing of Personal data, such as a joint Controllers agreement. If the UT has to provide Personal data in order to make use of the services of another party, whereby that party has an independent responsibility with regard to the Processing of that Personal data, the agreements will be laid down in a data sharing agreement.

6.9.3 TRANSFER OF PERSONAL DATA WITHIN THE EUROPEAN ECONOMIC AREA

The UT only transfers Personal data to a recipient (Processor, Controller or Third party) established within the EEA, if the Processing is based on one of the principles for data Processing from Article 6 (see paragraph 6.12) of the GDPR and if the recipient meets the legal requirements from the GDPR. If the Processing contains Special categories of personal data, Article 9 of the GDPR must also be complied with.

6.9.4 TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

In addition to the conditions that apply to the transfer of Personal data within the EEA, the UT applies the following additional conditions for transfer to recipients outside the EEA:

1. the third country, territory, specific sector in a third country, or the international organization in question offers an adequate level of protection according to the European Commission. The UT applies as an appropriate level of protection the general list of countries with an adequate level of protection published by the European Commission[14];
2. transfer takes place on the basis of appropriate safeguards from the GDPR, Articles 46 and 47. The UT uses the Standard Contractual Clauses (SCCs) as determined by the European Commission and additional security measures, which are assessed for each intended transfer;
3. Transfer takes place on the basis of one of the legal exceptions from Article 49 of the GDPR.

6.10 SECURITY

The UT ensures an adequate level of security and implements appropriate technical and organisational measures to protect Personal data against loss or against any form of unlawful Processing. These measures are also aimed at preventing unnecessary and unlawful collection and Processing of Personal data. The UT has implemented an Information Security Policy in which measures have been elaborated that are used within the UT[15].

When Personal data are Processed, a risk analysis of data protection and information security will be performed. Access to Personal data is given on a need-to-know basis and systems are designed and set up as much as possible according to the principles of Privacy by design and Privacy by default.

At the UT, all Personal data is classified as confidential. Everyone should be aware of the confidentiality of Personal data and act accordingly.

Anyone who becomes aware of Personal data is obliged to observe confidentiality. The duty of confidentiality does not apply if any legal regulation obliges them to disclose or the need to disclose arises from their duties.

6.11 RIGHTS OF DATA SUBJECTS

The GDPR provides Data subjects with certain rights that allow them to control the Processing of their Personal data. A request can be submitted by way of a form on the privacy website[16].

The following points apply to all rights of Data subjects detailed in this chapter:

Communication to the Data subject

The UT ensures that the information and communication is provided to the Data subject in an accessible and understandable manner and in clear and simple language. The language will be tailored to the target group.

Term

A request from a Data subject will be responded to in writing as soon as possible, but no later than one month after submission. The Data subject will in any case be informed of the action taken on the request. If the period of one month is not reasonably feasible, the Data subject will be informed of this

[14] See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[15] See: https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/policy-on-information-security.pdf
[16] See: https://www.utwente.nl/en/cyber-safety/privacy/your-privacy-rights/

within this period. In that case, the UT will comply with the request of the Data subject within two months after the first term has expired.

Identity of the Data subject

When providing the relevant information, the UT will ensure that the applicant's identity is properly established. The UT can request additional information for this purpose.

Minors

A request to exercise one of the rights as elaborated in this chapter by a Data subject who is a Minor, who has been placed under guardianship or for whom an administration or mentorship has been instituted, must be submitted by his legal representative. A response from the UT will also be sent to this legal representative.

6.11.1 RIGHT OF ACCESS

Request

Every Data subject has the right to inquire whether his Personal data is being Processed and, if this appears to be the case, the right to access the Personal data Processed concerning him. If the UT Processes a lot of data from the Data subject, the UT may request the Data subject prior to the provision of information to specify which information or which Processing activities the request relates to[17].

Statement

If Personal data are Processed, the communication from the UT contains an overview of the requested data, which may include:

- The Personal data itself;
- The purposes of the Processing;
- The categories of Personal data to which the Processing relates;
- The recipients or categories of recipients, in particular recipients in third countries or international organisations, if applicable;
- The retention period of the Personal data or the criteria for determining that period;
- Whether the Personal data is also used for automated decision-making. The underlying logic, as well as the relevance and expected consequences of the Processing for the Data subject must also be reported;
- The rights of the Data subject;
- The Data subject's right to lodge a complaint with the DPA;
- If the Personal data have not been obtained directly from the Data subject: the source of the Personal data.

Copy

The Data subject may request a copy of his Personal data. The UT is not always obliged to provide a copy[18].

A copy should be provided in a commonly used electronic format, unless the request is made on paper or the Data subject explicitly requests a paper copy.

Costs

[17] See amongst others number 63 in the preamble to the GDPR, Amsterdam District Court 20 June 2019 ECLI:NL:RBAMS:2019:4418, Den Bosch Court 1 February 2018 ECLI:GHSHE:2018:363 and Noord-Holland District Court 23 May 2019, ECLI:NL:RBNHO:2019:4283
[18] ECLI:NL:RBMNE:2020:5275

Each first copy can be requested free of charge. The UT may charge the Data subject a reimbursement of administrative costs for each additional copy.

Rights and freedoms of others

The UT will take into account the rights and freedoms of others when providing the Personal data. This can, for example, lead to the fact that when access to the Personal data of the Data subject is provided, the data that can be traced back to others is shielded or omitted.

6.11.2 RIGHT TO DATA PORTABILITY

Grounds for request

Every Data subject can submit a request to the UT to obtain his data in a structured, common and machine-readable form or to have it transferred directly to another Controller, without being hindered by the UT, if both of the following conditions are met:

1. The Processing by the UT is based on the legal ground of ‘consent’ or 'execution of an agreement with the Data subject'.
2. The Processing in question is fully automated.

Rights and freedoms of others

The UT 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 Processing for the performance of an agreement, the UT may not decide to delete the data. However, after the retention period has expired, the UT must still delete the data.

If the right has been exercised in the context of a Processing based on the consent of the Data subject, the UT may decide to delete the data after exercising the right.

6.11.3 RIGHT TO RECTIFICATION, ADDITION, ERASURE OR RESTRICTION OF PROCESSING

Request for rectification, addition, erasure or restriction

With regard to Personal data recorded about him, each Data subject can request the UT to rectify, add, erase or restrict the Processing of this data.

Notification

If it appears that the Processed Personal data of the Data subject are factually incorrect, incomplete or irrelevant for the purpose or purposes of the Processing or have otherwise been Processed in violation of a legal requirement, the Controller and/or the Processor shall improve, permanently delete, supplement or limit this data.

In addition, Third Parties to whom the data have been provided prior to rectification, addition, erasure or restriction will be notified, unless this is not reasonably possible or is not relevant given the circumstances. The applicant may request a statement from the person to whom the UT has made this notification.

Term for execution

The Controller ensures that a decision to rectification, addition, erasure or restriction is implemented as soon as possible.

6.11.4 RIGHT TO OBJECT

Grounds for objection

There are two grounds for Data subjects to object to Processing:

1. In connection with his or her personal circumstances, every Data subject may object to Processing at the UT if this Processing takes place on the basis of
    a. the fulfilment of a task of public interest or in the context of the exercise of the public authority of the Controller, or
    b. the fulfilment of the legitimate interest of the UT or of a Third party to whom the data is provided.

    In the event of an objection, the UT will in principle suspend the Processing. If the UT can demonstrate that its compelling legitimate interests outweigh the interests or fundamental rights and fundamental freedoms of the Data subject, the Processing will be continued. If the objection is justified, the UT will take (free of charge) measures that are necessary to stop Processing the Personal data for the purposes in question.
2. In the case of Processing for the purpose of 'direct marketing', a Data subject has the right to object at all times. In the event of an objection, the UT will immediately suspend Processing for direct marketing purposes.

6.11.5 AUTOMATED DECISION-MAKING

Grounds

Data subjects have the right not to be subject to a decision based solely on automated Processing, which has legal consequences for them. A “decision based on automated Processing” means a decision made without human intervention. This includes Profiling.

The UT may only make decisions based on automated Processing in the following three situations:

1. If the decision is necessary for the conclusion or performance of an agreement with the Data subject;
2. If the decision is authorised by 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 Data subject. This consent can be withdrawn at any time.

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

6.11.6 LEGAL PROTECTION

General complaints

If the Data subject is of the opinion that the legal provisions regarding privacy protection or the provisions of this Policy are not being correctly enforced towards him, he can submit a written complaint to the UT. Questions or complaints in connection with (the Processing of) Personal data can be reported to the DPO (dpo@utwente.nl).

Other objection options

In addition to the general internal complaints procedure, the Data subject has the following options if he feels that the UT has committed a violation of the GDPR that affects him:

A. Petition procedure before the court

If the UT has rejected a request as described in paragraph 6.12 of this Policy, or the UT has rejected the request of the Data subject, or has responded insufficiently in the opinion of the Data subject, the Data subject has, pursuant to Article 35 paragraph 2 GDPR Implementation Act the possibility to start a petition procedure with the court.

The petition must be submitted to the court within six weeks after receipt of the answer from the UT. If the UT has not responded to the request of the Data subject within the set term, the petition must be submitted within six weeks after the end of that term. The application does not have to be submitted by a lawyer.

B. Enforcement Request to the DPA

If the UT has rejected a request as described in section 6.12 of this Policy, or if the UT has rejected the Data subject's request, the Data subject has the option of submitting a complaint to the DPA or to an interest group. to act on his behalf.

6.12 ACCOUNTABILITY

The UT has taken several measures to demonstrate compliance with the legal requirements of the GDPR, including the implementation of this Policy.

6.12.1 REGISTER OF PROCESSING ACTIVITIES

The responsible party within the UT ensures that every (fully or partially automated) Processing of Personal data is included in the Register of Processing activities. The responsible party must contract the involved PCP or the DPO to do so. The DPO assesses the legal validity of the Processing. The DPO checks whether the establishment of the Register of Processing activities meets the requirements of Article 30 GDPR and is responsible for checking and monitoring the documentation/evidence of the registered Processing operations.

6.12.2 DATA PROTECTION IMPACT ASSESSMENTS / DATA TRANSFER IMPACT ASSESSMENTS

The UT also carries out a DPIA for (research) projects, infrastructural changes or the purchase of new systems that probably pose a high risk to the rights and freedoms of natural persons. The pre-DPIA can help determine if a full DPIA is needed[19]. If necessary, the UT can decide to carry out a DTIA. When drawing up a DPIA and/or DTIA, the DPO is asked for advice.

[19] See: https://www.utwente.nl/en/cyber-safety/privacy/pre-dpia-form/

7 DATA BREACHES

This chapter describes the policy regarding the reporting, registration and handling of Data breaches or the presumption of a Data breach.

7.1 DATA BREACH

A Data breach is a breach of the security of Personal data, which accidentally or unlawfully leads to any unauthorised Processing thereof. This could be, for example, the theft of a laptop, a lost USB stick, incorrectly issued authorisation or an e-mail sent to the wrong person. All Data breaches or suspected Data breaches must be reported internally to CERT-UT: cert@utwente.nl. Some Data breaches must be reported to the DPA and in some cases also to the Data subject(s). The assessment of whether a report is made to the DPA rests with the EB on the advice of the DPO. Reporting to the DPA must take place within 72 hours of discovery and is done by the DPO.Reporting and registering

7.2 NOTIFICATION AND REGISTRATION

A Data breach at the UT may arise within the own organization, but also at a UT-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 UT's reporting point on cert@utwente.nl.

A notification of a (possible) Data breach should be made immediately after discovery, even if it is not yet certain whether there is a Data breach or if information is still missing.

If possible, the following information must be provided 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 UT: 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 the DPO in a register.

7.3 HANDLING

In the case of a Data breach, this is handled as described in the procedure for handling Data breaches[20].

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.

[20] See: https://www.utwente.nl/en/cyber-safety/reportincident/procedure-for-handling-data-breaches.pdf

8 TO CONCLUDE

The Policy is evaluated and if necessary updated each year.

The Policy is written in Dutch and translated into English. In case of any discrepancies, the Dutch version will prevail.

For questions or remarks regarding this Policy, please contact the DPO (dpo@utwente.nl).