UNIVERSITY OF TWENTE.

Reference: SB/UIM/15/0901/khv
Date: 10 October 2016

Status: Definitive
Date established by the Board: 17 October 2016
Author: Wim Koolhoven/Jan Evers

Privacy policy University of Twente

The University of Twente's privacy policy is in line with the Model Policy on the Processing of Personal Details in Higher Education. This model has been drawn up by the SURF Project Group 'Preparation for the Implementation of the General Data Protection Regulation' and SURFibo[1], and published under the Creative Commons[2] licence.

Where substantial, specific additions for the University of Twente have been made, the text is displayed in grey and explained if necessary.

[1] Information security officers and privacy officers employed in higher education consult each other in SCIPR (SURF Community for Information Security and PRivacy, previously SURFibo). The objective is to improve the information security and privacy at universities of applied sciences and traditional universities. SCIPR does this for instance through the development of policy and guidelines.
[2] See http://creativecommons.org/licenses/by/3.0/nl/deed.en

University of Twente privacy statement

The University of Twente respects the private lives of students, staff, and others. Information is not stored for longer than necessary for the purpose for which it has been collected and is not used for purposes that are inconsistent with this. The University of Twente processes personal data in accordance with the Dutch Personal Data Protection Act (Wbp) and the European General Data Protection Regulation (Avg).

Personal data are collected for the purposes of the administration of education and operational management, such as name, email address, telephone number, home address, details about previous and current education, study progress, and details relating to other student and personnel matters. These details are provided by the persons concerned themselves, but can also be sourced from third-party systems, for instance the Dutch tax department (Belastingdienst), Studielink, the Immigration and Naturalisation Service (IND), and the ABP pension fund.

Via the website data is collected, primarily for the purposes of student recruitment, such as registrations for open days or requests for information.

The University of Twente only provides personal data to third parties if there is a legal basis for this.

Data for academic research are collected in accordance with the codes of conduct of the Association of Universities in the Netherlands (VSNU) and Federa (Federa is a cooperative venture between researchers in health care), where necessary following assessment by the faculty ethics committee if available and reporting to the Data Protection Officer.

When processing the personal data in operational management, research, and the administration of education, the University of Twente works on the basis of the principle of proportionality: the processing of personal data must be proportional to the intended operational or research objective. A good assessment takes place in order to find the right balance between privacy and the research goal.

There is adequate protection for personal data, and they are handled with as much care as possible. Attention is devoted to privacy within all processes and activities. To this end, Privacy Contact Persons (PCPs) have been appointed within all service departments and faculties. They hold regular consultations with the Data Protection Officer.

The present privacy policy provides students, staff, and other concerned persons with insight into how privacy is taken care of at the University of Twente.

Researchers at the University of Twente are investigating privacy and related topics. Use is made of this knowledge in setting up and implementing the policy.

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 operational management. The Dutch Personal Data Protection Act (Wbp) was recently extended with the addition of an obligation to disclose data breaches, and at European level the General Data Protection Regulation (Avg) was recently adopted as the successor to the current directive on which the Personal Data Protection Act is based. There are therefore reasons enough for the University of Twente to draw up a privacy policy.

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.

Definitions and abbreviations are included in Appendix A.

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 standard and to allocate the tasks, powers, and responsibilities within the organization clearly and consistently.
- 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 Framework of Legal Standards for Cloud Services in Higher Education[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.

1.2 Creation of the policy

In 2015, the IT Board discussed privacy on two occasions and made guidance statements for the formulation of a privacy policy.

In the autumn of 2015, participants were sought via I-Beraad (owners of university systems), the ICT quarterly consultation (ICT representatives of faculties), University Operations Committee (UCB), and ICT-SO (student consultative body) for a working group. The policy has been formulated with that working group on the basis of the national model of SURF and the guidance statements of the IT Board.

Representatives of the Facility Service Centre (FSC), the Marketing & Communications department (M&C), Library, IT Services & Archive (LISA), Geo-Information Science and Earth Observation (ITC), Engineering Technology (ET), Institute for Innovation and Governance Studies (IGS), Strategy & Policy (S&P), and the Student Union participated in the working group. In addition, interviews were held with a number of scientists and people involved in ethical committees. The Privacy Contact Persons (PCPs) of the service departments that did not participate in the working group were involved in the process via the PCP consultative body. The draft policy has been assessed externally by Kienhuis-Hoving.

The policy has been further refined in consultation with the chairman of the IT Board and then submitted to the Executive Board for adoption with positive advice from the IT Board.

The adoption and publication of the European General Data Protection Regulation took place before the conclusion of the policy formulation so that the policy could still be assessed against the definitive version of the General Data Protection Regulation.

[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 taskforce Cloud, adopted by the board of the Platform ICT & Bedrijfsvoering (ICT and Operational Management Platform) on 3 April 2014, retrievable via www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/legal-standards-framework-for-cloud-services

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 the Dutch Personal Data Protection Act (Wbp).
- Personal data are only processed for explicitly described and justified purposes. These purposes are formulated in concrete terms prior to the processing.
- When processing personal data, the quantity and the type of data remain limited to the personal data that are necessary for the specific purpose. The data needs to be adequate with an eye to that objective, as well as serving the issue at hand and not being excessive.
- The processing of personal data takes place in the least drastic manner and should be in reasonable proportion to the intended purpose.
- Measures are taken in order to guarantee as far as possible that the personal data to be processed are correct and up to date.
- Personal data are kept adequately secure in accordance with the applicable security standards.
- Personal data are not processed further in a way that is inconsistent with the purposes for which they were obtained.
- 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.
- Every person concerned has a legal right to inspect, correct, supplement, remove, or protect the personal data relating to them in the individual processing types, and in certain cases has the right to object.
- For all records that are not strictly necessary for a business process, a clear so-called opt-out will be offered to the person concerned as far as this is technically possible.

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 codes for scientific research are also applied and adhered to.

3.2 Personal Data Protection Act

The University of Twente has implemented the statutory requirements (including 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) by means of the privacy policy.

3.3 Public Records Act

The University of Twente adheres to the provisions relating to the retention periods as set out in the Public Records Act, for example, and the Public Records Decree regarding the manner in which information recorded in documents (digital or otherwise), information systems, websites, etc. must be handled.

3.4 Telecommunications Act

Amongst other things, the Telecommunications Act describes the rules that cookies on websites must satisfy.

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. This is also known as ‘portrait right’.

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.

In research, the responsibility lies with the researcher, the research team leader, and the faculty concerned.

4.1 Overlap with information security

The Information Security Officer[6] and the Information 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 has final responsibility for the lawful and careful processing of personal data within the University of Twente and establishes the policy, the measures, and the procedures in the field of processing 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 has final responsibility 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 Data Protection Officer supervises the application of and compliance with the privacy legislation. The statutory duties and powers of the Data Protection Officer give this official an independent position within the organization.

The Data Protection Officer advises and informs the entire organization and the individual units regarding the application of the privacy legislation. The Data Protection Officer takes care of the information provision on the processing of personal data to employees, students, and managers. The Data Protection Officer promotes the privacy awareness of employees and students, for instance through the maintenance of a privacy portal on the website of the University of Twente. An annual privacy report is drawn up each year.

The Data Protection Officer is the point of contact and expert for those with questions about the protection of personal data and manages the index of reports of the processing of personal data.

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 Information Security Manager is set out in the Information Security Policy.
[8] See the University of Twente Information Security Policy, reference SB/UIM/15/0106/khv, www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/informatiebeveiligingsbeleid-engels-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 or director of operations is responsible for the implementation of the privacy policy within his or her unit. The director is also responsible for personal data that are entered into an institute system from his/her unit.

The director 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

In consultation with the University Operations Committee (UCB), a decision was made in 2015 to appoint a Privacy Contact Person (PCP) per unit (faculty/service department) in order to provide support for the tasks of the Data Protection Officer. The Privacy Contact Person maintains contact with the Data Protection Officer and advises the unit regarding privacy. The Privacy Contact Person has the following tasks:

- ensuring that the data processing is reported to the Data Protection Officer;
- taking care of awareness and training;
- acting as a privacy expert within their own unit;
- ensuring that a Privacy Impact Assessment is performed for all new data processing;
- coordinating with the service department director or director of operations regarding privacy matters;
- being involved with the handling of data breaches and other incidents on behalf of the unit.

The Privacy Contact Person can be supported in this by the Data Protection Officer. If a faculty does not appoint a Privacy Contact Person, the director of operations takes on this role.

[9] See also the memorandum 'Houderschap van een instellingssysteem', reference SB/UIM/15/2801/EVS, http://www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf (only available in Dutch)

For a consistent, university-wide performance of the privacy policy, the Privacy Contact Persons and the Data Protection Officer ensure that they are familiar with each other's tasks. They inform and support each other.

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. This has been further elaborated in the data policy of the unit concerned or of the University of Twente.[10]

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.

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. 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 but, to the extent that it falls within the Exemption Decision[11], should be reported directly to the Dutch Data Protection Authority.

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

[10] See www.utwente.nl/en/service-abc/!/product/p885008/research-data-management
[11] Under certain circumstances, frequently occurring standard processing that is generally known to take place does not need to be reported. See autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp (only available in Dutch)

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 Personal Data Protection Act. 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 institute, 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. See chapter 4, Roles and responsibilities with regard to the processing of personal data.

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.

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 aspects (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 a privacy portal on the University of Twente website.

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 Security Officer, and the Security Managers.

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 employees 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

6.1 Basis, purpose limitation, and balancing of interests

The processing of personal data must be based on one of the legal bases as described in article 8 of the Personal Data Protection Act. The responsible party describes in advance the purposes for the processing. These purposes are formulated in concrete and specific terms. For every processing, an assessment is made of the extent to which the processing of the personal data is necessary. The various interests are weighed up against each other and the effectiveness, proportionality, and subsidiarity are examined. Personal data are not processed further in a way that is inconsistent with the purposes for which they were obtained.

The University of Twente takes the necessary measures in order to ensure that personal data are correct and accurate in view of the purposes for which they are collected or are subsequently processed.

For research projects and other projects, infrastructural modifications, or the purchase of new systems, account is taken of privacy from the start by means of a Privacy Impact Assessment (PIA).

In the implementation, the University of Twente adheres to the principles of ‘Privacy by Design’ and ‘Privacy by Default’.

6.2 Reporting and documenting processing

The fully or partially automated processing of personal data should be reported to the Data Protection Officer of the University of Twente. The Data Protection Officer assesses the legal validity of the registration and ensures adequate documentation.

The processing is sufficiently documented and published on media that is accessible to the persons concerned with a statement of the objective of the registrations and the responsibilities.

6.3 The organization of the security

The University of Twente ensures an adequate level of security and implements appropriate technical and organizational measures in order to protect personal data against loss or any form of unlawful processing. These measures also aim to prevent the unnecessary and/or unlawful collection and processing of personal data.

A risk analysis of privacy protection and information security forms part of the internal risk management and control system of the University of Twente.

6.4 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.

6.5 Retention periods / destruction periods per type of data

Personal data are not retained for longer than necessary for the purposes for which they have been collected or are to be used. After the expiry of the retention period,[12] 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.

6.6 Special personal data

In principle, the processing of special personal data is prohibited, unless there is a legal basis, explicit permission from the person concerned, or a compelling reason in the general interest. More stringent requirements for the protection of these personal data also apply. Where the basic protection is inadequate, individually tailored additional measures must be taken for each information system.

Special personal data include details relating to a person's religion/faith or life principles, race, political persuasion, health, sex life, membership of a trade union, and criminal record.

6.7 Transfer of personal data to third parties

6.7.1 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.

6.7.2 Transfer of personal data within the European Union

The University of Twente only provides personal data to third parties if there is a legal basis for this transfer.

Special personal data are not provided to third parties without the explicit permission of the person concerned.

6.7.3 Transfer of personal data outside the European Union (including the EEA)

The University of Twente only provides personal data to third parties located in a country outside the European Union if that country as a whole or the company/institute concerned within that country *guarantees an appropriate level of security*. For countries with an appropriate level of security, the University of Twente makes use of the list of countries published by the European Commission[13].

The University of Twente only provides personal data to countries without an appropriate level of security on the basis of a legal exception as referred to in article 77 of the Dutch Personal Data Protection Act. One of the exceptions is 'unambiguous permission': the party whose personal data are transferred has granted unambiguous permission for this. Another legal exception is transfer on the basis of a model contract (such as those drawn up by the European Commission). In the case of changes or additions to the model contract, a permit from the Minister of Security and Justice is required. In all cases, if personal data are transferred to a country outside the European Union, it is compulsory to report this to the Dutch Data Protection Authority.

[12] 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.
[13] For this list, see autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu (only available in Dutch)

6.7.3.1 Third parties to which the University of Twente transfers personal data (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

7 Incidents relating to personal data

Every complaint or report relating to the processing of personal data within the University of Twente is a privacy incident. The best-known form of such an incident is a data breach[14].

This chapter describes the policy relating to the reporting, registration, and handling of incidents or suspected incidents in standard operational management and in exceptional circumstances.

7.1 Reporting and registering

Employees of the University of Twente are obliged to report any data breaches or suspected data breaches and other privacy incidents immediately. For the sake of efficiency, incidents should preferably be reported via CERT-UT[15] or the LISA service desk. If the reporter so prefers, this can also be done confidentially via the Privacy Contact Person (PCP) or the Data Protection Officer (DPO); they will keep the name of the reporter confidential. Examples of data breaches are contained in Appendix B .

Records are kept of all incidents and how they were dealt with by CERT-UT. Reports are dealt with confidentially. The reporter can be confident that submitting a report will not have any personal consequences for them. As long as the incident has not yet been dealt with, the reporter must handle the report confidentially and not communicate anything about it to those concerned or other parties.

7.2 Handling

The handling of incidents has the objective of resolving the problem, limiting the damage, and complying with the legislation. Normally, the Information Security Manager[16] is the person who assesses whether there is likely to have been a data breach. In that case, the Data Protection Officer and the Privacy Contact Person at least will be involved in the further handling of the matter. Often, the manager concerned will also become involved. The Data Protection Officer is responsible for dealing with privacy incidents.

If the incident relates to a data breach, then the Dutch Data Protection Authority[17] rules will be used to determine whether reporting to the Data Protection Authority is compulsory. The report will be coordinated with the Executive Board. A report must be submitted to the Dutch Data Protection Authority without delay, and within 72 hours after detection.

Once the persons concerned have been compulsorily informed in line with the rules of the Dutch Data Protection Authority or in an alternative manner if so desired, communication takes place in consultation with the Marketing & Communications department. The reporter is informed of how the incident has been dealt with.

7.3 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.

---

[14] If personal data fall into the hands of third parties that are not permitted to have access to those details, this is referred to as a data breach.
[15] Computer Emergency Response Team of the University of Twente. See also the information security policy.
[16] The role of the Information Security Manager is set out in the Information Security Policy.
[17] The obligation to disclose data breaches is contained in the Dutch Personal Data Protection Act. There are policy rules for the application of article 34a of the Dutch Personal Data Protection Act.
See https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken (only available in Dutch)

Appendix A 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).

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

Processor: the person who processes the personal data for the benefit of the person responsible, without being subject to that person's direct authority.

CERT-UT: Computer Emergency Response Team of the University of Twente; see Information Security Policy.

EB: Executive Board

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.

Director of Operations: Director of operations of a faculty

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 Protection Officer (DPO): Official responsible for data protection

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

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

PIA: Privacy Impact Assessment

Privacy by default: When users are offered the choice between various options, the standard setting gives the best privacy guarantees.

Privacy by design: The management of the entire life cycle of personal data, from their collection to their processing and removal, whereby systematic attention is devoted to all-encompassing guarantees relating to accuracy, confidentiality, integrity, physical safety, and the removal of the personal data.

Privacy Impact Assessment (PIA): A tool that helps with the identification of privacy risks and provides guidance in reducing these risks to an acceptable level.

UT: The University of Twente

UCB: University Operations Committee

Responsible person/party: the natural person, legal entity, or any other party or management body that, either alone or together with others, determines the objective and the means for the processing of personal data. At the University of Twente, the Executive Board is responsible, but this responsibility is delegated to the owner of the relevant information system.

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.

Personal Data Protection Act: The Dutch Personal Data Protection Act, based on Directive 95/46/EC. Referred to as the Wbp (Wet bescherming persoonsgegevens).

Appendix B 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 photocopier;
- anonymous survey results that can nevertheless be traced to identifiable respondents;
- access to personal data (that can be traced to natural persons) 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.

Appendix C Privacy rules

In sub-fields, specific privacy rules are necessary. Employees can limit themselves to the privacy rules that are relevant to them. Through the formal establishment of these privacy rules, the implementation is made verifiable.

In the following sub-fields, specific privacy rules have been established:

1. *Inventory of data processing*
2. *Website and apps*
3. *Scientific research*
4. *Administration and operational management*
5. *CCTV (Closed-Circuit TV)*
6. *Key issues regarding confidentiality*

Privacy rules – Inventory of data processing

Introduction

The privacy policy indicates that specific privacy rules are necessary in sub-fields. One of these sub-fields relates to the production of an inventory of data processing.

Responsibility

1. Data processing is to be reported to the Data Protection Officer in accordance with article 27 of the Dutch Personal Data Protection Act and article 30 of the General Data Protection Regulation.
2. The system owner, supported by the Privacy Contact Person, ensures that the data processing is reported.
3. The Data Protection Officer takes care of an inventory of the reports of data processing.

Reports

4. Every report comprises at least the following details:
    - Functional name of the system;
    - Owner of the system;
    - External parties involved;
    - Objective of the processing;
    - Which categories of personal data are recorded for which categories of persons;
    - The retention periods to be adhered to, which can differ per type;
    - Which special personal data[18] are recorded;
    - Description of the security measures taken;
    - List of organizations to which personal data are provided.
5. The objective of the processing also states the legal basis:
    - Permission of the person concerned;
    - The performance of an agreement;
    - A legal obligation;
    - The protection of a vital interest of the person concerned;
    - The performance of a public-law task;
    - The justified interest of the responsible person/party or a third party to whom details are provided.
6. The Data Protection Officer takes care of the quality control of the reports.
7. Information systems that do not use personal data are not reported.
8. Processing that falls under the Exemption Decision[19] are nevertheless reported to the Data Protection Officer as much as possible for the purposes of the overview.
9. An overview of the reports is published by the Data Protection Officer on the website.

[18] The processing of personal details relating to a person's religion/faith or life principles, race, political persuasion, health, sex life, membership of a trade union, and criminal record, which is only permitted under certain conditions; see Dutch Personal Data Protection Act, section 2.

[19] From a legal point of view, under certain circumstances, frequently occurring standard processing that is generally known to take place does not need to be reported. Exemption Decision, Dutch Personal Data Protection Act, Dutch Bulletin of Acts, Orders and Decrees 2014, 520 (entering into force on 7 May 2001), see http://wetten.overheid.nl/BWBR0012461 (only available in Dutch). As the University of Twente does want an overview of all processing, an internal report is desired.

Privacy rules – Website and apps

Introduction

The privacy policy indicates that specific privacy rules are necessary in sub-fields. One of these sub-fields related to the websites and apps of the University of Twente.

Responsibility

1. The Marketing & Communications department is responsible for the implementation of the privacy policy on the websites and in apps.
2. Websites on subdomains[20] fall under the responsibility of the unit or association concerned. The Marketing & Communications department proactively advises them.
3. The Marketing & Communications department informs website administrators about the relevant privacy rules when they collect personal information using forms.

Tracking visitors

4. Visitors are only tracked if there is a good reason to do so. The principle of proportionality is applied in this regard.
5. The websites and apps clearly indicate how and with which goals visitors are tracked.
6. The websites and apps clearly indicate which data is collected.
7. The websites and apps clearly indicate how visitors can visit the website or use the app without being tracked.

Forms

8. Forms on the websites and in apps do not ask for more personal information than is necessary for the purpose for which it is being collected.
9. Every form clearly specifies the purpose or purposes for which the requested information is to be used.
10. Every form is part of an information system to which the 'Privacy rules – Inventory of data processing' apply.

IP addresses

11. IP addresses are not used to track visitors.
12. IP addresses are logged and can be used to resolve security incidents and/or technical malfunctions.
13. IP blocks can be used for statistical analysis.

[20] According to the name policy for websites and email addresses at the University of Twente www.utwente.nl/nl/sb/beleidsterreinen/universitair-informatiemanagement/voor-eindgebruikers/namenbeleid_ict_domeinen_ut.pdf (only available in Dutch), subdomains are possible, for instance for associations, projects, and events.

Privacy rules – Scientific research

Introduction

The privacy policy indicates that specific privacy rules are necessary in sub-fields. One of these sub-fields relates to scientific research. Researchers like to have a clear overview of the privacy rules relevant to them. This overview is provided below. These rules also apply to students.

If a faculty has an ethics committee, the recommendation is to involve the Privacy Contact Person in the review process.

Relevant documents

1. Every researcher who works with personal data must take cognizance of the VSNU Code of Conduct (Association of Universities in the Netherlands) for the use of personal data in scientific research.[21]
2. Every researcher who works with medical data must take cognizance of the Federa Code of Conduct for health research.[22]
3. Consult the website of LISA regarding Research Data Management.[23]

Start of research

4. In accordance with the research data policy, a data management plan is drawn up.
5. If identifying data of persons are used, a report is submitted to the Data Protection Officer in consultation with the Privacy Contact Person, in line with the 'Privacy rules – Inventory of data processing'.
6. Consider anonymization, or - if that is not possible - the use of pseudonyms for data.[24]
7. Clear agreements are made on how to deal with personal data. These are recorded in the data management plan.

Data storage

8. If use is made of external storage or other cloud services, a processor agreement[25] is entered into.
9. Consider that personal data cannot be stored outside the EU without strict conditions being met.
10. Prevent data breaches by using data storage with care.
11. Whenever confidential information is transported (for instance on a USB stick or laptop), encryption is to be used.
12. Whenever confidential information is provided to others (for instance via a cloud service or by email), encryption is to be used.
13. For access to a data repository, the Authorization policy[26] is applied.

---

[21] See www.vsnu.nl/en_GB/code-personal-data
[22] See federa.org/sites/default/files/bijlagen/coreon/code_of_conduct_for_medical_research_1.pdf
[23] See www.utwente.nl/en/service-abc/!/product/p885008/research-data-management
[24] Article 89 subsection 1 of the General Data Protection Regulation: … If those purposes can be accomplished through further processing that does not allow the identification of persons concerned (or no longer allows that), they must be accomplished in that manner.
[25] LISA can provide support in this regard. See also www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/legal-standards-framework-for-cloud-services
[26] See www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)

Privacy rules – Administration and operational management

Introduction

The privacy policy indicates that specific privacy rules are necessary in sub-fields. One of these sub-fields relates to the administration and operational management. The Security rules – Information systems that are included as an appendix in the Information Security Policy[27] apply in full.

Responsibility

1. The holder[28] or owner of an information system is responsible for compliance with the privacy rules.

Acquisition

2. Before or at the start of the project, a classification takes place in line with the *Classificatierichtlijn Informatie en Informatiesystemen* (Classification guideline on information and information systems)[29] so that the results can help determine the requirements for the information system.
3. When using cloud services, the SURF *Juridisch normenkader cloudservices hoger onderwijs*[30] (Legal standards framework for cloud services in higher education) is applied.
4. If personal data is processed, a Privacy Impact Assessment (PIA) is performed. The results of this are included in the business case for the project. An assessment takes place regarding the extent to which the processing of personal data is necessary. The various interests are weighed up against each other in this regard.
5. Ideally, the Data Protection Officer is present and/or involved in the performance of the PIA. In any case, the result is sent to the Data Protection Officer for assessment.
6. If an external processor is called upon, a processor agreement[31] is entered into.

Implementation

7. The principles of 'Privacy by Design' and 'Privacy by Default' are adhered to. Amongst other things, this means that account must be taken of privacy from the very start of the design process, and that data minimization must be applied.
8. The owner reports the data processing to the Data Protection Officer before the system is put into use.
9. Retention periods are determined so that personal data are not kept for longer than is necessary.
10. Persons concerned are informed by the owner about the data processing.
11. The owner sets up a process so that the right to inspect, correct, supplement, remove, or protect the personal data can be satisfied in good time, within four weeks.

---

[27] See www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/informatiebeveiligingsbeleid-engels-def.pdf
[28] See also www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf (only available in Dutch)
[29] See www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/classificatierichtlijn-ut.pdf (only available in Dutch)
[30] See www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/legal-standards-framework-for-cloud-services
[31] The legal standards framework of SURF includes a model processor agreement.

12. For test purposes, in principle no production data is used, except for the reproduction of observed problems. If production data is used for an acceptance test, the authorization matrix must be the same as that of the production environment.

Privacy rules – CCTV (Closed-Circuit TV)

Introduction

The privacy policy indicates that specific privacy rules are necessary in sub-fields. Aside from the 'Privacy rules – Administration and operational management', the rules set out below also apply to CCTV at the University of Twente.[32]

Responsibility

1. As the owner of the CCTV, the Facility Service Centre is responsible for compliance with the privacy rules at the University of Twente.

Objective and transparency

2. The data is used exclusively for the following purposes:
   a. Protection of the safety and health of natural persons;
   b. Security of access to buildings and sites;
   c. Monitoring of items located in buildings or on sites;
   d. Registering incidents.
3. Cameras are installed in a clearly visible way or the use of CCTV is indicated on location by means of stickers, for instance.

Access

4. The live images are only accessible for the staff members responsible for security and monitoring at the University of Twente.
5. Access to recorded images is only possible in a specially set-up room.
6. Only the head of the responsible department and their deputy have access to recorded images.
7. The staff members involved have a duty of confidentiality with regard to data that can be traced to persons.

Storage

8. Recorded camera images are saved and stored in such a way that they are not accessible for others.
9. Recorded camera images are kept for no longer than two weeks. Camera images recorded at the instructions of the University of Twente Security Services are kept for a maximum of four days.

Incidents

10. After an incident, a decision can be made once it is clear that relevant images are available to preserve these images and to save them for as long as is necessary for the relevant investigation.
11. In the event that there is a reasonable suspicion of a prohibited or unlawful action, use can be made of concealed cameras without the persons concerned being informed following a written instruction to do so from the Executive Board.

[32] For the use of CCTV by the University Security Services, the University of Twente CCTV Regulations 2011, https://www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/cameratoezicht.pdf (only available in Dutch), provide a further elaboration of these privacy rules.

12. Images are only provided to third parties if the interest of the University of Twente requires this following a decision to that effect by the Executive Board. The police can only be given images after submitting a demand or after permission is granted by the public prosecutor or acting public prosecutor.

Privacy rule – Key issues regarding confidentiality

In early 2015, a memorandum was published - 'Omgaan met Vertrouwelijkheid' (Dealing with confidentiality) - by a working group of the I-Beraad, the consultation group of owners of university systems. This memorandum aims to provide handy suggestions for holders of information and information systems that need to make decisions regarding whether or not to take measures.

The most important element of this memorandum is a list of concrete key issues. This list is shown below, almost unchanged. These generic key issues will need to be translated per data processing process.

1. *Authorization*. It is important to be sure that only those persons who actually require the confidential information have access to it. Implementation of the Authorization policy[33] can take care of this. Being alert to the use of an account of someone else, including in cases of temporary substitution such as maternity leave.
2. *Authentication*. Prevent anyone from being able to pass themselves off as someone else and thus gain access to confidential information. Prevent staff from sharing or writing down passwords. Consider two-factor authentication.
3. *Access* from locations other than the permanent workplace. Working from home or working at a different location can give rise to extra risks. This can be prevented by filtering on the basis of IP address.
4. *Entering* data. Consider that notes and temporary documents can also contain confidential information. Ensure the controlled disposal or destruction of such papers and files.
5. *Processing* and consultation of data. When a staff member requests or adds information, confidential information can be concealed or moved to a screen for which an additional button needs to be used, if this confidential information is not required for the action.
6. *Interruption* of the work. Consider the use of screensavers and do not leave confidential papers lying in view.
7. *Exchanging* data with other systems. Do not exchange more data than necessary. When confidential information is provided, make sure that the data will remain confidential. Make clear agreements in advance.
8. *Production* of reports. It is necessary to determine for each report the extent of confidentiality that applies. If it is known that a report is confidential, this can be stated on the report as standard.
9. *Saving* data. Critical confidential information should be stored in encrypted form. In the case of central storage, this is important in order to prevent hackers or administrators gaining access. In the case of decentralized storage, the risks posed by theft and viruses form a greater threat. Paper featuring critical confidential information, such as a dossier, must be stored in a locked cupboard.
10. *Storing* email. The storage of confidential information in the email system means that this information remains accessible for a long period of time via any device, including smartphones and tablets. This could include records of staff reporting sick, letters of application, and annual performance appraisal results. Delete emails containing confidential information as soon as possible.
11. *Archiving* information. Determine the retention period and the rules relating to access and destruction.
12. *Printing* data. Paper featuring critical confidential information may only be printed if the staff member is present by the printer, and it must not be left lying around or taken off the

[33] Authorization policy of the University of Twente, reference SB/UIM/13/0819/khv, see http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)

premises without appropriate measures being taken, and after use it must be disposed of or destroyed in a controlled manner.

13. *Carrying* digital data. Information can be carried on a USB stick, a hard disk, a laptop, etc. Consider first whether all the information needs to be carried and whether the confidential information could be omitted. Critical confidential information should be stored in encrypted form.
14. *Consulting* information on mobile devices. As described in the memorandum 'Gebruik van "eigen" apparatuur en applicaties' (Use of 'own' devices and applications)[34], extra security measures can be taken independent of the classification.
15. *Working* in public spaces. Other people can read information from the screen or from paper, for instance over someone's shoulder. Prevent this when consulting confidential information. Places where this could be a risk include: corridors, cafeteria, cafés, restaurants, waiting rooms, trains, aeroplanes, etc.
16. *Discussing* information. When discussing information, including over the phone, be aware that other people could be listening in.
17. *Sending* information. Check whether the person you are contacting actually needs this information, and try to minimize the amount of information provided. Check whether we as the University of Twente are allowed to provide this information to that person. When confidential information is sent by email or in another digital form, it must be encrypted.
18. *Audit trail*. It must be possible to ascertain by means of a log file who has had access to which confidential information.
19. *Theft* of information. If paper featuring confidential information or an information carrier (USB stick, tablet, etc.) is lost, which procedures apply? On the one hand, you should minimize further damage by modifying passwords etc. What else needs to be done is elaborated in the procedure 'Obligation to disclose data breaches'.
20. *Writing* procedures. Include the roles of staff in procedures but not the names of individuals.
21. *Expansion* or redesign/purchase of new applications. Consider in advance which security aspects play a role. The Classification guideline and a PIA can assist in this regard. Getting halfway through a project with extra requirements brings about higher costs.
22. *Testing* applications. When testing an application, the live data is often used as it is so realistic. However, for most tests the critical confidential information can easily be omitted. This can be done by overwriting certain fields in a database with other information or by garbling the information, and by not using any original confidential documents.
23. *Outsourcing* work or making use of cloud services. Make clear agreements and if personal data are exchanged, enter into a processor agreement.

[34] 'Gebruik van "eigen" apparatuur en applicaties', reference SB/UIM/12/1018/khv, see www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gebruik-van-eigen-apparatuur-en-applicaties-en-1.pdf