Universiteit Utrecht

Utrecht University Personal Data Processing Policy

Utrecht, 30 May 2018 23:13:00
Version number: UU-1.0

Universiteit Utrecht

Publication details

This policy document of Utrecht University is modelled on the SURF Utrecht University Personal Data Processing Policy

SURF
PO Box 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

The version of the model policy that has been used is an update of the Joint Product of the SURF Project Group 'Preparation for Implementation of the General Data Protection Regulation' and SURFibo (now SCIPR). Frans Pingen (Wageningen University), Bart van den Heuvel (Maastricht University) Sedat Capkin (SURFsara), Ronja Meijer (Wageningen University) Jaap Gall (HAN University of Applied Sciences) and Chloë Baartmans (SURFnet) were involved in drafting the original version.

Version 2.0 March 2018

SURF is the ICT collaborative organisation of Dutch higher education and research.
The digital version of this publication is available on the SURF website: www.surf.nl/publicaties

Universiteit Utrecht

Contents

Universiteit Utrecht

1. Introduction

Storage and Processing of Personal Data is required for the business processes of education and research institutions. It must be done with the greatest possible care, because abuse of Personal Data can cause major harm to students, employees and other Data Subjects at Utrecht University, but also to Utrecht University itself.
Therefore, Utrecht University attaches great value to the protection of the Personal Data provided to it and to the manner in which Personal Data are processed. The correct processing of Personal Data is the responsibility of the Executive Board of Utrecht University.

By describing the measures in this policy document, Utrecht University aims to take and takes its responsibility of optimising the quality of the processing and the security of Personal Data and, in doing so, complying with the relevant privacy laws and regulations.

1.1. Definitions

GDPR: General Data Protection Regulation[1].

Policy: this policy concerning the processing of Personal Data by Utrecht University.

Data Subject: an individual and natural person to whom Personal Data pertains.

Controller: the Executive Board of Utrecht University, which determines the objective and the means of the Processing or Personal Data.

Personal Data: all data concerning an identified or identifiable natural person.

Processor: a (third) party engaged by Utrecht University that processes Personal Data for the benefit of Utrecht University, based on the latter's written instructions.

Processing: every act or series of acts relating to Personal Data, which includes collecting, recording, organising, storing, consulting, updating, blocking, deleting or destroying data.

Third party: every other party, not being the Data Subject, the Controller or the Processor, or any person who is under the direct control of the Controller or the Processor and is authorised to process Personal Data.

Data leak: a breach of the security of Personal Data, leading to any form of unlawful Processing thereof. This includes both deliberate and accidental data leaks.

Privacy by Default: data processing with the standard settings of products and services set in such a way that it provides maximum protection of the privacy of Data Subjects. This means – among other things – requesting and processing as little data as possible.

Privacy by Design: The management of the entire life cycle of Personal Data, from the collection to the processing and erasure, with mechanisms that are designed to take as much account of the privacy of Data Subjects as possible. This involves systematically paying attention to comprehensive safeguards with regard to accuracy, confidentiality, integrity, physical security and erasure of the Personal Data.

[1] The General Data Protection Regulation came into effect on 25 May 2016 and entered into force on 25 May 2018.

Privacy Impact Assessment: An assessment that aids in identifying privacy risks and provides points of reference for bringing these risks down to an acceptable level.

Profiling: any form of automated Processing of Personal Data in which, based on Personal Data, certain personal aspects of a natural person are evaluated, a particular objective of which is to analyse or predict his professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or relocations.

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

1.2. Extent and objective of the Policy

The Policy concerns the processing of Personal Data of all Data Subjects at Utrecht University, which in any case includes all employees, students, guests, visitors and external relations (hired/outsourcing), as well as other Data Subjects of whom Utrecht University processes Personal Data.

In this Policy, the emphasis is on the full or partial computerised/systematic processing of Personal Data that takes place under the responsibility of Utrecht University, as well as on the documents on which such processing is based, which are kept in a file. In addition, the Policy applies to all non-computerised processing of Personal Data that are included in a file or that are intended to be included in a file.

At Utrecht University, the protection of Personal Data is interpreted broadly. There is an important relationship and partial overlap with the adjoining policy area of information security, which is about availability, integrity and the reliability of data, including Personal Data. At a strategic level, attention is paid to these areas of overlap, and both from a systematic and from a substantive point of view, the policies are coordinated as much as possible.
The Policy of Utrecht University serves to optimise the quality of the Processing and the security of Personal Data, while trying to find the right balance between privacy, functionality and security.

The goal is to respect the private life of the Data Subject as much as possible. The data that pertains to a Data Subject must be protected against unlawful and unauthorised use or misuse on the basis of the fundamental right to protection of one's Personal Data. In this connection, the processing of Personal Data must meet relevant laws and regulations and Personal Data must be safe with Utrecht University.

Concretely, the objective of the Policy for Utrecht University is the following:

- Providing a framework: the Policy provides a framework for the testing of (future) Processing of Personal Data to an established 'best practice' or standard, and to lay down the duties, powers and responsibilities within the organisation.
- Setting standards: the basis for the security of Personal Data is ISO 27001[2]. Measures are taken on the basis of 'best practices' in higher education and on the basis of ISO 27002[3].
- The SURF Legal Standards Framework (Cloud) Services[4] is used as a best practice for cloud services and other outsource contracts.
- The taking of responsibility: by the Executive Board by laying down the starting principles and the organisation of the processing of Personal Data for the entire organisation/Utrecht University.

[2] In full: NEN-ISO/IEC 27001: Requirements for Management Systems for information security.
[3] In full: NEN-ISO/IEC 27002: Code for Information Security.
[4] SURF Legal System of Standards (Cloud) Services, laid down by the board of Platform ICT & Bedrijfsvoering on 3 April 2014 and updated in 2016, which can be found at://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html

- Decisive implementation of the policy by making clear choices with regard to measures, and actively monitoring the implementation of the policy measures.
- Complying with Dutch and European legislation.

In addition to the above concrete objectives, a more general objective is to create awareness of the importance of and need for protecting Personal Data, in part to avoid risks associated with not complying with the relevant laws and regulations.

2. Policy principles for the Processing of Personal Data

2.1. Policy principles

A general policy principle is that Personal Data must be processed in accordance with the relevant laws and regulations, and that it must be done properly and carefully. There must be a good balance between the interest of Utrecht University to process Personal Data and the interest of the Data Subject to have their private life respected and be able to make their own choices with regard to their Personal Data, in a free environment.

In order to comply with the above policy principle, the following principles apply:

- Processing of Personal Data must be based on one of the statutory bases as referred to in Article 6 of the GDPR ('lawfulness').
- Personal Data may only be processed fairly and in a transparent manner in relation to the Data Subject. This means that it must be clear to Data Subjects to which extent and how Personal Data are processed. Information and communication about this must be easily accessible and understandable ('fairness and transparency').
- Personal Data may only be processed for specified, explicit and legitimate purposes. It concerns specific and justified purposes that must have been laid down and described before the Processing starts. Personal Data may not be Processed in a manner that is not in line with the purposes for which these were collected ('purpose limitation').
- When Processing Personal Data, the amount and the type of data will be limited to the Personal Data that is required for the specific purpose. The Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- The Processing of Personal Data may not be too drastic and must be in a reasonable proportion to the intended purpose ('data minimisation').
- Measures are taken to ensure, to the extent possible, that the Personal Data to be processed are accurate and up-to-date ('accuracy').

Personal Data will be appropriately secured according to the current security standards ('integrity and confidentiality'). Personal Data may be processed for no longer than is necessary for the purposes of the Processing. The applicable retention and destruction terms are taken into account ('storage limitation').

3. Laws and regulations

At Utrecht University, the relevant laws and regulations are dealt with as follows.

3.1. Dutch Higher Education and Research Act (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*)

Utrecht University has a quality assurance system, which safeguards – among other things – the careful handling of details in the student administration and the study results. In addition, codes of conduct and integrity codes for academic and non-academic staff are complied with and applied.

3.2. General Data Protection Regulation

Utrecht University has implemented the statutory requirements (which includes lawful and careful processing of Personal Data and taking appropriate technical and organisational measures against loss and unlawful Processing of data or Personal Data) by means of the Policy.

3.3. Dutch Public Records Act (*Archiefwet*)

Utrecht University complies with the provisions of the Dutch Public Records Act concerning the manner in which information laid down in documents (digital or otherwise), information systems, websites, etc. is to be handled. This is part of the annual external audit reports.

3.4. Dutch Telecommunications Act (*Telecommunicatiewet*)

The measures Utrecht University has taken to comply with the privacy laws are also sufficient to safeguard the protection of the personal life of users on our public networks. The regulations of the Dutch Telecommunications Act or any replacement laws concerning legal interception and the retention obligation have been implemented separately.

4. Roles and responsibilities with regard to the Processing of Personal Data

In order to ensure that Personal Data is processed in a structured and coordinated manner, Utrecht University recognises a number of roles that have been assigned to officials of the existing organisation.

4.1. Executive Board

The Executive Board is the Controller and, as a result, bears ultimate responsibility for the lawful and careful Processing of Personal Data at Utrecht University and will determine the policy, the measures and the procedures in the field of the Processing.

4.2. Portfolio holder for security of Personal Data

The portfolio holder for security of Personal Data is the board member who has privacy in his portfolio. He bears ultimate responsibility for the security of Personal Data within Utrecht University.

4.3. Data Protection Officer

Utrecht University will appoint an internal supervisor for the Processing of Personal Data. This supervisor is referred to as the Data Protection Officer (hereinafter referred to as: 'the DPO'). Utrecht University will involve the DPO in all matters involving Personal Data in a timely manner. The statutory duties and responsibilities of the DPO give this officer an independent position at Utrecht University.
Utrecht University will register the DPO with the supervisory authority.

The duties of the DPO will in any case include:

- informing and advising all the parties involved about their obligations under the GDPR;
- monitoring compliance with the GDPR and other relevant privacy legislation;
- monitoring Utrecht University's compliance with this privacy policy;
- ensuring that a Privacy Impact Assessment is performed;
- collaborating with the supervisory authority;
- serving as the main point of contact for the supervisory authority.

4.4. System owner

The system owner is responsible for ensuring that the application and the associated IT facilities support the process for which he is responsible properly and comply with the Policy. This means that the system owner must ensure that, both now and in the future, the application meets the requirements and needs of the users and complies with laws and regulations.

4.5. Manager

Creating awareness of and compliance with the Policy is part of the integrated business operations. Every supervisor is charged with:

- seeing to it that his employees are familiar with the Policy;
- ensuring that his employees comply with the Policy;
- periodically discussing the subject of privacy at work meetings.

5. Implementation Policy

The Executive Board of Utrecht University is responsible for the Processing of Personal Data, with regard to which it determines the objective and the means. It is considered the **Controller** within the meaning of the GDPR. However, the actual Processing of Personal Data takes place at various levels of Utrecht University. The proper, efficient and responsible management of an organisation is often referred to as governance. It predominantly refers to the relationship with the most important interested parties of Utrecht University, such as the owners, employees, students, other clients and society as a whole. A good corporate governance policy protects the rights of all Data Subjects.

5.1. Division of the responsibilities

- The careful processing of Personal Data must be viewed as a **first line responsibility**: this means that the supervisors bear primary responsibility for the careful Processing of Personal Data in their section or department. This includes the choice of measures and the implementation and enforcement thereof. The line responsibility also includes the duty to communicate the policy with regard to the Processing of Personal Data to all the relevant parties.
- Careful handling of Personal Data is **everyone's responsibility**. Employees and students are expected to behave ethically. It would not be acceptable if deliberate or accidental behaviour were to lead to situations that result in loss of and/or damage to the image of Utrecht University or individuals. For that reason, codes of conduct have been drawn up and implemented.

5.2. Incorporation in the institutional governance / Coordination with adjoining policy areas

In order to correctly reflect the cohesion within the organisation with regard to data protection and coordinate the initiatives and activities in the field of Personal Data Processing within the various sections, it is important that the subject of privacy is discussed at various levels, in a structured manner.

At a **strategic level**, governance and compliance are defined, as are the objectives, scope and ambition in the field of privacy aspects.

At a **tactical level**, the strategy is translated into plans, standards to be applied, and evaluation methods. These plans and instruments are a guideline for the implementation.

At an **operational level**, matters that concern the day-to-day business operations (implementation) are discussed.

5.3. Awareness and training

Policies and measures are not sufficient to exclude risks in the field of the Processing of Personal Data. At Utrecht University, awareness must be continuously tightened, so that knowledge of risks is increased, and safe and responsible behaviour is encouraged. Part of the Policy are regularly recurring awareness campaigns for employees, students and guests. These campaigns may be in line with national campaigns within higher education, and where possible in line with other security campaigns. An increase in the awareness is the responsibility of the supervisors, supported by the Data Protection Officer, the privacy contact persons, the Corporate Information Security Officer and the Local Information Security Managers.

5.4. Supervision and compliance

Audits allow you to check the effectiveness of the Policy and the measures taken. The DPO will initiate the supervision of the lawful and careful processing of Personal Data, in collaboration with the Information Security Officer and the internal auditor.

Any external checks are performed by independent accountants. This is linked to the annual audit and will, to the extent possible, be coordinated with the regular Planning & Control cycle.

Should compliance with the protection of data and privacy details be seriously lacking, Utrecht University may impose a sanction on the responsible employees, within the frameworks of the CLA and the statutory possibilities.

The processing of Personal Data is a continuous process. Technological and organisational developments within and outside of Utrecht University require us to check periodically whether the Policy still suffices.

6. Lawful and careful Processing of Personal Data

Utrecht University processes Personal Data in accordance with the principles as laid down in paragraph 2.1 of this Policy. In implementing these principles, Utrecht University takes the measures described in this chapter.

6.1. Basis

Utrecht University only processes Personal Data if one of the legal bases as referred to in Article 6 of the GDPR applies:

a. Consent of the Data Subject.
b. Required for the performance of an agreement with the Data Subject.
c. Required to meet a statutory obligation of the Controller.
d. Required to protect the vital interests of the Data Subject or another natural person.
e. Required for the performance of a task carried out in the public interest or in the exercise of an official authority.
f. Required for the purposes of the legitimate interests of the Controller or a third party.

6.2. Privacy statement

Utrecht University only processes Personal Data fairly and in a transparent manner in relation to the Data Subject. This means that Utrecht University will inform the Data Subject of the extent to which and the manner in which his Personal Data are processed. When collecting the Personal Data, Utrecht University will inform the Data Subject by means of a privacy statement. The information will be provided before the Processing takes place, unless this is not reasonably possible. For further information, please refer to paragraph 8 of this Policy.

6.3. Retention period

Personal Data is not stored for longer than is required for the purposes for which they are collected or used. After the retention period[5], Personal Data must be removed from the active administration.
After the retention period lapses, Utrecht University will destroy the Personal Data or, if the Personal Data are intended for historical, statistical or scientific purposes, keep them in an archive.

6.4. Appropriate security measures

Utrecht University will provide an adequate level of security and implement appropriate technical and organisational measures to secure Personal Data against loss or any form of unlawful Processing. These measures are intended to – among other things – prevent the unnecessary or unlawful collection and Processing of Personal Data. Utrecht University has implemented an internal security policy containing measures that Utrecht University employees apply.

A risk analysis of privacy protection and information security is part of the Utrecht University's internal risk management and supervision system.

[5] Retention periods may be determined by law, as is the case with financial details or formal study results, but may also be laid down by Utrecht University, for example in an agreement between Utrecht University and the Data Subjects.

6.5. Obligation to document

Utrecht University has taken various measures to show that it meets the statutory requirements of the GDPR, which includes implementation of this Policy.

In addition, all fully or partially computerised Processing of Personal Data must be reported to the DPO of Utrecht University. The DPO will assess the lawfulness of the Processing and will see to adequate documentation of all the relevant details.

In addition, Utrecht University will perform a Privacy Impact Assessment of research or other projects, infrastructural changes or the purchase of new systems that are likely to pose a significant risk for the rights and freedoms of natural persons. If this shows that the Processing would pose a significant risk if Utrecht University does not take measures to reduce that risk, Utrecht University will consult the supervisory authority before any processing takes place.

6.6. Privacy by Design and Privacy by Default

In the implementation of all Processing, Utrecht University uses the principles of 'Privacy by Design' and 'Privacy by Default'.

6.7. Confidentiality

At Utrecht University, all Personal Data is classified as confidential. Everyone should be aware of the confidentiality of Personal Data and act accordingly.

Even those who are not already bound by a duty of confidentiality by virtue of their office or profession or by statutory regulation, are obliged to keep the Personal Data that they become aware of confidential, except insofar as a statutory regulation obliges them to make such information public or the need to make such information public arises from their duties.

6.8. Special Personal Data

In principle, processing special Personal Data is forbidden, unless one of the statutory exceptions of the GDPR applies, which includes – among other things – 'express consent of the Data Subject' and 'reasons of substantial public interest'. In addition, the security of special Personal Data is subject to stricter requirements. Where the basic security is not sufficient, individually adjusted additional measures must be taken for each information system.

Special Personal Data includes the following data:

- details showing a person's racial or ethnic origin;
- political opinions;
- religious or ideological beliefs;
- details showing whether someone is a member of trade union;
- genetic data for the purpose of uniquely identifying a natural person;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health;
- details concerning to a person's sex life or sexual orientation.

Two types of Personal Data do not fall under the category of special Personal Data, though the Processing and security thereof are subject to strict requirements:

a. Personal Data on criminal convictions and offences may only be processed under government supervision or when authorised by European or national legislation.
b. Under Dutch law, national citizen service numbers (the so-called BSN or the education number) may only be processed if this is stipulated by law.

6.9. Transfer of Personal Data

6.9.1. Subcontracting the Processing to a Processor

If Utrecht University has Personal Data processed by a Processor, the execution of the Processing is provided for in a processor's agreement between Utrecht University, the Controller and the relevant Processor.

6.9.2. Transfer of Personal Data within the European Economic Area (hereinafter referred to as 'the EEA')

Utrecht University only provides Personal Data to a Processor established within the EEA, if the processing is based on one of the bases for data processing of Article 6 or Article 9 of the GDPR and if the Processor meets the legal requirements of the GDPR.

6.9.3. Transfer of Personal Data outside of the EEA

Utrecht University only provides Personal Data to Processors in a country outside of the EEA if one of the following conditions has been met:

1. The third country, area, specified sector in a third country or the international organisation in question offers an adequate level of protection according to the European Commission.

   To determine whether the level of protection is adequate, Utrecht University uses:
   - The general list of countries with an adequate level of protection as published by the European Commission[6];
   - The Privacy Shield for companies in the United States, published by the European Commission in collaboration with the US Department of Commerce[7].

2. Transfer takes place on the basis of **appropriate safeguards** of the GDPR, Article 46 and 47.

3. Transfer takes place on the basis of one of the **legal exceptions** of Article 49 of the GDPR.

6.10. Questions and complaints procedure

6.10.1. Reports and registration

Questions and complaints in connection with the processing of Personal Data can be reported to the DPO (privacy@uu.nl). Questions or complaints with a significant or potentially significant impact will be recorded in a register.

Questions and complaints can be reported by anyone, including Data Subjects, Processors or Third Parties.

[6] This can be found at the following link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[7] This can be found at the following link https://www.privacyshield.gov/list.

6.10.2. Weak points in the security

Employees will register and immediately report weak spots in the systems or services to the CERT (cert@uu.nl). All reports on the relevant weak spots in the security will be recorded in a register.

6.10.3. Handling

Questions, complaints and weak spots in the security will be reported to the responsible department or person and subsequently dealt with according to the established procedures, as soon as possible.
If the Personal Data of Data Subject(s) or the company processes, the finances or good reputation of Utrecht University are in serious jeopardy, the Executive Board and the DPO will in any case be informed.

6.10.4. Evaluation

It is important to learn from the feedback that is provided through the questions and complaints procedure. Registration of significant questions, complaints and weak spots, and a periodical report on these aspects form part of processing Personal Data in a professional manner. The reports on this will therefore be a fixed part of the annual report of the Executive Board and – if applicable – that of the DPO.

7. Data leak

This chapter describes the policy with regard to reporting, registering and handling a Data Leak or a suspected Data Leak as part of the regular business operations and in special circumstances.

7.1. Data leak

A Data Leak is a breach of the security of Personal Data, leading to any form of unlawful Processing thereof. This may include – for example – the theft of a laptop, a flash drive that has been left on the train or an email that has been sent to the wrong person. Data leaks must be reported to the supervisory authority within 72 hours of discovery thereof and, in some cases, to the Data Subject as well.

7.2. Report and registration

A Data Leak can arise both within Utrecht University's own organisation, and with a Processor that has been engaged by Utrecht University. The following situations must be distinguished:

a. Employee: if they detect or suspect a (potential) Data Leak, or suspect that they are part of a Data Leak themselves, employees must contact the CERT (cert@uu.nl).
b. *Processor*: a Data Leak may also arise with a Processor that has been engaged by Utrecht University. The Processor will report the Data Leak to Utrecht University in accordance with the applicable processor's agreement.
c. *Other persons*: if someone other than an employee or a Processor detects or suspects a Data Leak or potential Data Leak or is part of a Data Leak himself, he can also contact the CERT (cert@uu.nl).

A Data Leak or potential Data Leak must be reported as soon as possible. The following data must be provided when a Data Leak is reported:

- Who has made the report?
- What has been reported?
- Where has the report come from?
- What data (details) are involved?
- How did the incident take place?
- Which systems were involved/affected by the incident?
- When did the incident take place?
- If the report was made by an employee of Utrecht University: what has been done to resolve the incident/prevent such an incident in the future?

Every Data Leak and the handling thereof will be recorded in a register.

7.3. Handling

If there has been a Data Leak, it will be handled in accordance with the specific provisions on Data Leaks as contained in the relevant laws and regulations, as described in the policy rules on the duty to report data leaks of the Dutch Data Protection Authority[8], so that the report of a Data Leak reaches the right people and, eventually, the supervisory authority and Data Subjects in time.

[8] Policy rules for data breach notification obligation of the Dutch Data Protection Authority: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

If the Personal Data of Data Subject(s) or the company processes, the finances or good reputation of Utrecht University are in serious jeopardy, the Executive Board and – if applicable – the DPO will in any case be informed.

7.4. Decision-making

After a (potential) Data Leak has been reported in accordance with the preceding paragraphs, the CERT will issue advice on the obligation to report it to the supervisory authority and the Data Subject. The DPO will consider this advice. The DPO will subsequently decide on whether to make the report or not.

7.5. Evaluation

It is important to learn from Data Leaks to reduce the likelihood of future Data Leaks. Registration of Data Leaks and a periodical report on that form part of processing Personal Data in a professional manner. The reports on Data Leaks concerning Personal Data will therefore be a fixed part of the annual report of the Executive Board and that of the DPO.

8. Rights of Data Subjects

The GDPR gives Data Subjects certain rights that allow it to control the Processing of their Personal Data. A request may be submitted to the DPO (privacy@uu.nl or via the usual postal address: Utrecht University, attn. the Data Protection Officer, PO Box 80125, 3508 TC Utrecht).

The following applies to all the rights of Data Subjects as laid down in this chapter:

- *Report to the Data Subject*

Utrecht University will see to it that the information provided to and the communication with the Data Subject is concise, accessible and understandable, using clear and simple language. The language will be adjusted to the target group.

- *Term*

A request of a Data Subject will be responded to as soon as possible, though no later than within four weeks of its submission, in writing. The Data Subject will at least be informed of what action will be taken on the request. If the four-week term is not reasonably practicable, the Data Subject will be informed of that within this term.
In such case, Utrecht University will comply with the Data Subject's request within two months of the first term.

- *Identity of the Data Subject*

When providing the relevant information, Utrecht University will ensure that the identity of the applicant is properly established. To this end, Utrecht University may request additional information.

- *Minors*

A request for exercise of one of the rights as laid down in this chapter by a minor Data Subject, or a Data Subject who has been placed under guardianship or for the benefit of whom an administration or mentorship has been instituted, must be made by the Data Subject's legal representative. Utrecht University's response will be sent to this legal representative as well.

8.1. Right to information

The Data Subject has the right to have Utrecht University inform him of certain aspects of the Processing of his Personal Data.
Utrecht University will inform the Data Subject free of charge of the Processing of his Personal Data, both in the situation in which the Personal Data is collected from the Data Subject directly, and in the situation in which these are collected via a different route.

A. Collection directly from the Data Subject

Prior to the collection of the data, Utrecht University will at least provide the Data Subject with the following information if the data have been collected from the Data Subject directly:

- The identity and contact details of the Controller and – where appropriate – the DPO.
- The specific objectives of the Processing for which the Personal Data are intended, as well as the legal basis of the Processing.
- The legitimate interests of the Controller or Third Party if the Processing is based on the legal ground of 'legitimate interest'.
- Where appropriate, the Controller's intention to transfer the Personal Data to a third country, which country this is and on which basis the Personal Data will be sent there.
- The period for which the Personal Data will be stored or, if this is not possible, the criteria used to determine that period.
- The existence of the right to apply to the Controller for inspection, rectification or deletion of Personal Data and restriction of the processing that pertains to him, as well as the right to object against the Processing and the right to data portability.
- The right to submit a complaint to the Supervisory authority.

- The recipients or categories of recipients of the Personal Data.
- If the Processing is based on 'consent', the Data Subject's right to revoke that consent at all times.
- Whether the Personal Data are required for the performance of an agreement or to comply with a statutory obligation.
- Whether the Personal Data are also used for computerised decision-making. In addition, the underlying logic, as well as the interest and the expected consequences of the Processing for the Data Subject are indicated.

B. Collection other than directly from the Data Subject

If the Personal Data have been collected via a different route rather than from the Data Subject himself, the Data Subject will be provided with the following information, in addition to the above:

- The categories of Personal Data.
- The source the Personal Data came from.

This information will be provided as soon as possible, though no later than within four weeks of the data being provided, or upon the first contact with the Data Subject.

8.2. Right to inspection

- *Request*

Every Data Subject has the right to ask whether his Personal Data are processed and, if this is the case, the right to inspection of the processed Personal Data that pertains to him.

- *Notification*

If data are processed, the notification of Utrecht University will contain a full overview of the following data:

- A description of the purposes of the Processing.
- The categories of data to which the Processing pertains.
- Categories of recipients.
- Available information on the source of the data.
- The retention period for data or, if that is not possible, the criteria used to determine that period.
- The right of Data Subject to request that the Controller rectify or delete data or restrict the Processing, or to object to the Processing, as well as the right to data portability.
- The right of the Data Subject to submit a complaint to a supervisory authority.
- All the available information on the source of the data, if the data was not collected from the Data Subject.
- Whether the Personal Data are also used for computerised decision-making. In addition, the underlying logic, as well as the interest and the expected consequences of the Processing for the Data Subject are indicated.
- The appropriate safeguards that are in place, if the data are transferred to a third country.

- *Copy*

The Data Subject may request a copy of all Personal Data. This copy must be provided in a common electronic form, unless the request was made on paper or the Data Subject expressly requests a paper copy.

- *Costs*

Every first copy can be requested free of charge.

- *Rights and freedoms of others*

When providing the data, Utrecht University will take account of the rights and freedoms of others.

8.3. Right to data portability

- *Grounds for request*

Every Data Subject can submit a request to Utrecht University to obtain his data (free of charge) in a structured, common and machine-readable form, or to have this transferred directly to another Controller, without being hindered by Utrecht University, if the following conditions are met:

1. The Processing by Utrecht University is based on 'consent' or 'performance of an agreement with the Data Subject'.
2. The Processing in question is entirely computerised.

- *Rights and freedoms of others*

When providing the data, Utrecht University will take account of the rights and freedoms of others.

- *Removal of details*

If a Data Subject has exercised his right to data portability within the framework of Processing in the performance of an agreement, Utrecht University may not decide to delete the data. However, after the retention period has lapsed, Utrecht University must delete the data after all.

If the right has been exercised within the framework of Processing on the basis of consent of the Data Subject, Utrecht University may decide to delete the data after the right is exercised.

8.4. Right to rectification, supplementation, erasure or restriction of the Processing

- *Request for rectification, supplementation, erasure or restriction*

Every Data Subject may request with regard to the Personal Data Utrecht University has recorded about them that these data be corrected, supplemented or erased, or that the Processing thereof be restricted. For the right of rectification, the Personal Data are temporarily blocked and no longer processed by Utrecht University. The block will be clearly indicated in the file.

- *Notification*

If it turns out that the Personal Data of the Data Subject that have been recorded are factually incorrect, incomplete for the purpose or objectives of the Processing or are not relevant or have otherwise been processed in violation of a legal provision, the data manager (which may be both the functional manager or the Processor) will correct, permanently erase, supplement or restrict these data.

In addition, Third Parties to whom the Data were provided prior to the rectification, supplementation, erasure or restriction will be informed of this, unless this is not reasonably possible or not relevant in view of the circumstances. The applicant may request an overview of those to whom Utrecht University has made this announcement.

- *Term for implementation*

The data manager will ensure that a decision to correct, supplement, erase or block is implemented as soon as possible. The implementation thereof will be at no cost to the Data Subject.

8.5. Right of objection

- *Grounds for objection*

For Data Subjects, there are two grounds for objecting to Processing:

1. In connection with his or her personal circumstances, any Data Subject may object to the Processing at Utrecht University, if this Processing takes place based on a) the provision of a service of public interest or within the framework of the public authority of the Controller, of b) the representation of the legitimate interests of Utrecht University or of a Third Party to whom the details are provided. For a description of the bases, see paragraph 6.1.

In principle, Utrecht University will stop further Processing in the event of an objection. If Utrecht University can show that its compulsory legitimate interests outweigh the interests or basic rights and fundamental freedoms of the Data Subject, Processing will resume. If the objection is justified, Utrecht University will take the measures required to no longer process the Personal Data for the relevant purposes (free of charge).

2. If the objective of the Processing is 'direct marketing', a Data Subject will be authorised to object at all times.

In the event that a Data Subject objects to this, Utrecht University will stop processing Personal Data for direct marketing purposes and will not resume the processing (free of charge).

8.6. Computerised decision-making

- *Grounds*

Data Subjects have the right to not be subjected to decisions that are solely based on computerised Processing, if that decision has legal consequences for them. A 'decision based on computerised Processing' must be understood to refer to a decision taken without human intervention. This includes – among others – Profiling.

Only in the following three situations may Utrecht University decide on the basis of computerised Processing:

1. If the decision is required in entering into or performing an agreement with the Data Subject.
2. If the decision is allowed under a European or national law, provided that this law provides for adequate measures to protect the rights and freedoms and legitimate interests of the Data Subject.
3. If the decision is based on the express consent of the Data Subject. This consent can be revoked at all times.

In all the situations as described above, Utrecht University will take adequate 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 Utrecht University, the right of the Data Subject to express his views, and the right to dispute the decision. Minors will never be subjected to computerised decision-making.

8.7. Legal protection

- *General complaints*

If the Data Subject is of the opinion that the statutory provisions for the protection of privacy or the provisions of these regulations are not correctly complied with in his case, he can submit a written complaint to the DPO (privacy@uu.nl or via the usual postal address: Utrecht University, attn. the Data Protection Officer, PO Box 80125, 3508 TC Utrecht).

- *Other options for objection*

In addition to the general complaints procedure as described above, the Data Subject has the following options if the Data Subject feels that Utrecht University has violated the GDPR in a manner that affects him:

A. Application proceedings with the subdistrict court

If Utrecht University has rejected an application as described in paragraph 8.1 through 8.6 of this Policy, or Utrecht University has rejected the Data Subject's request, the Data Subject has the option of instituting application proceedings with the subdistrict court.

The subdistrict court must have received this application within six weeks of receipt of Utrecht University's reaction. If Utrecht University has not responded to the Data Subject's request within the

term set, the application must be submitted within six weeks of the end of that term. The application does not have to be submitted by a lawyer.

B. Objection and appeal

If Utrecht University has rejected a request as described in paragraph 8.1 through 8.6 of this Policy, or Utrecht University has rejected the Data Subject's request, and this decision of Utrecht University can be considered a decision of an administrative body within the meaning of Section 6, subsection 4 of the Dutch General Administrative Law Act (*Algemene wet bestuursrecht – Awb*), the Data Subject has the option of starting an objection procedure. An objection procedure must always be instituted within 6 weeks of a decision of Utrecht University being announced. A decision on appeal can be appealed with the court.

C. Request for enforcement to the supervisory authority

If Utrecht University has rejected an application as described in paragraph 8.1 through 8.6 of this Policy, or Utrecht University has rejected the Data Subject's request, the Data Subject has the option of submitting a complaint to a supervisory authority, or have an interest group act on his behalf.

Universiteit Utrecht

Conclusion

This policy was laid down by the Executive Board of Utrecht University on 29 May 2018.
A review of the policy is part of the annual plan-do-check-act cycle of Utrecht University. This also includes a check of the effectiveness of the measures.

Amendments of this policy are announced on the intranet and the most recent version has been published on www.uu.nl/privacy.

For questions or remarks with regard to this policy, please contact the DPO (privacy@uu.nl or via the usual postal address: Utrecht University, attn. the Data Protection Officer, PO Box 80125, 3508 TC Utrecht).