Privacy statement HU University of Applied Sciences Utrecht

Utrecht, May 2018

Version number: 1.0

Privacy statement HU University of Applied Sciences Utrecht 1.0

Table of Contents

1 Introduction

The storage and Processing of Personal Data is required for the business processes of educational and research organisations. Personal Data must be processed with the utmost care because misuse of Personal Data may substantially harm students, employees and other Data Subjects at HU University of Applied Sciences Utrecht, but also HU University of Applied Sciences Utrecht itself. That is why HU University of Applied Sciences Utrecht attaches a lot of value to the protection of the Personal Data that it receives and the way in which Personal Data is processed. The correct processing of Personal Data is the responsibility of the board of HU University of Applied Sciences Utrecht. By describing the measures in this Privacy Statement, HU University of Applied Sciences Utrecht intends to and accepts its responsibility to optimise the quality of the processing and the protection of Personal Data and as such, to comply with the relevant legislation.

1.1 Definitions

GDPR: The General Data Protection Regulation[1].

Supervisory authority: the Dutch Data Protection Authority

Policy: this policy in connection with the processing of Personal Data by HU University of Applied Sciences Utrecht.

Data subject: an individual and a natural person who Personal Data relates to.

Controller: the Executive Board of HU University of Applied Sciences Utrecht, which stipulates the purpose and resources of the Processing of Personal Data.

Personal Data: every detail about an identified or identifiable natural person.

Processor: a (third) party engaged by HU University of Applied Sciences Utrecht who processes personal data for HU University of Applied Sciences Utrecht and on the basis of the latter's written instructions.

Processing: every act or set of acts with regard to Personal Data, including the collection, recording, arranging, storage, consultation, editing, blocking, deletion or destruction of data.

Third Party: every person other than the Data Subject, the Controller or the Processor or any person who falls under the direct control of the Controller or the Processor and who is authorised to process Personal Data.

Data Breach: a breach of the security of Personal Data, resulting in any unauthorised Processing thereof. This includes both intentional and unintentional data breaches.

Privacy by Default: the processing of Personal Data during which the default settings of products and services are such that the privacy of Data Subjects is guaranteed to a maximum extent. Among other things, this means that the amount of data that is requested and processed is kept to a minimum.

Privacy by Design: The management of the entire life cycle of Personal Data, from collection to processing and removal, with mechanisms that are designed in such a way that they take the privacy of the Data Subjects into account to the greatest possible extent. Systematic attention is paid to all-encompassing safeguards with regard to accuracy, confidentiality, integrity, physical protection and the removal of the Personal Data.

Privacy Impact Assessment: An assessment that helps to identify privacy risks and that offers tools to reduce these risks to an acceptable level.

Profiling: every form of automated processing of Personal Data, in the course of which personal data is used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

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

[1]The General Data Protection Regulation came into effect on 25 May 2018

.

1.2 Scope and object of the Privacy Statement

The Policy relates to the processing of Personal Data of all Data Subjects at HU University of Applied Sciences Utrecht including, in any case, all employees, students, guests, alumni, those choosing a study programme, visitors and external customers (hire/outsourcing), as well as other Data Subjects whose personal data is processed by HU University of Applied Sciences Utrecht.

The Policy focuses on the full or partial automated/systematic processing of Personal Data under the responsibility of HU University of Applied Sciences Utrecht, as well as on the underlying documents included in a file. This Policy also applies to the non-automated processing of Personal Data which forms a part of a file or is intended to form a part of a file.

HU University of Applied Sciences Utrecht applies a broad interpretation to the protection of Personal Data. There is a significant relationship and partial overlap with the adjacent policy field of data protection, which concerns the availability, integrity and confidentiality of data, including Personal Data. On a strategic level, attention is paid to these areas of overlap and both systematic and substantive coordination is sought. The Policy at HU University of Applied Sciences Utrecht serves to optimise the quality of the Processing and the protection of Personal Data, finding the right balance between privacy, functionality and security.

The aim is to respect the privacy of the Data Subject to the greatest possible extent. The data that relates to a Data Subject must be protected against unlawful and unauthorised use or misuse on the basis of the fundamental right to the protection of his/her Personal Data. This means that the processing of Personal Data has to comply with relevant legislation and that Personal Data is safe at HU University of Applied Sciences Utrecht.

HU University of Applied Sciences Utrecht's object of the statement is, specifically, this:

- To offer a framework: the Policy provides a framework in order to verify the (future) Processing of Personal Data against a confirmed best practice or standard; and to assign the duties, powers and responsibilities to the organisation.
- To stipulate standards: the basis for the protection 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 System of Standards for (Cloud) services[4] is used as a best practice for cloud services and other outsourced contracts.
- To take responsibility: by the Executive Board, by documenting the basic principles and the organisation of the processing of Personal Data for the entire HU University of Applied Sciences Utrecht.
- Decisive implementation of the policy by making clear choices in terms of measures and by applying active monitoring of the implementation of the policy measures.
- To be compliant with Dutch and European legislation.

Apart from the aforementioned specific objectives, a more general objective is to create awareness of the importance of and the need to protect Personal Data, also in order to prevent risks caused by non-compliance with the relevant legislation.

[2] In full: NEN-ISO/IEC 27001: Requirements attached to Management Systems for information security

[3] In full: NEN-ISO/IEC 27002: Code for Information Security

[4] The SURF Legal System of Standards for (Cloud) services is stipulated by the board of the ICT & Management Platform of 03 April 2014 and it was updated in 2016. You can find it on https://www.surf.nl/kennisbank/2013/surfjuridisch-normenkader-cloudservices.html.

2 Policy principles of the Processing of Personal Data

2.1 Policy principles

The general policy principle is that Personal Data is processed properly and prudently, in accordance with the relevant legislation. There should be a good balance between the interests of HU University of Applied Sciences Utrecht to process Personal Data and the interests of the Data Subject to respect his privacy and to make his own choices about his Personal Data, in a free environment.

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

- The Processing of Personal Data is based on one of the statutory bases referred to in Article 6 of the GDPR ("lawfulness").
- Personal Data is processed only in a way that is correct and transparent with regard to the Data Subject. This means that it has to be clear to the Data Subjects to what extent and how Personal Data is processed. The information and communication about this has to be simple, accessible and comprehensible ("respectability and transparency").
- Personal Data is processed only for well-defined, explicitly described and legitimate purposes. It concerns specific and legitimate purposes that are documented and described before the Processing starts. Personal Data is not Processed in a way that is incompatible with the purposes for which it is obtained ("purpose limitation").
- During the Processing of Personal Data, the amount and type of data is limited to the Personal Data that is required for the specific purpose. With a view to that purpose, the data has to be sufficient, relevant and not excessive ("minimum data processing").
- Personal Data is processed according to the least invasive method and should be in reasonable proportion to the intended purpose ("minimum data processing").
- Measures are taken in order to offer the highest guarantee that the Personal Data to be processed is correct and up to date ("correctness").

Personal Data is properly protected in accordance with the prevailing protection standards ("integrity and confidentiality"). Personal Data is not processed for any more than is necessary for the purposes of Processing. The relevant retention and destruction terms are observed ("storage limitation").

3 Legislation

AT HU University of Applied Sciences Utrecht, the relevant legislation is dealt with as follows.

3.1 The Higher Education and Scientific Research Act

HU University of Applied Sciences Utrecht has a quality care system in place, which guarantees the prudent processing of data in the registration system and of study results. In addition, codes of conduct and integrity for scientific and non-scientific staff are observed and applied.

3.2 The General Data Protection Regulation

HU University of Applied Sciences Utrecht has implemented the statutory requirements (including the lawful and prudent processing of Personal Data and taking appropriate technical and organisational measures against loss and unlawful Processing of Personal Data) by means of the Policy.

3.3 The Public Records Act

HU University of Applied Sciences Utrecht abides by the regulations set out in the Public Records Act and the Public Records Decree about the way in which information recorded in (digitalised) documents, information systems, websites, etc. must be dealt with.

4 The roles and responsibilities with regard to the Processing of Personal Data

In order to structure and coordinate the Processing of Personal Data at HU University of Applied Sciences Utrecht, a number of roles are allocated to officers in the existing organisation.

4.1 The Executive Board

The Executive Board is the Controller and as such, the party that bears ultimate responsibility for the lawful and prudent Processing of Personal Data at HU University of Applied Sciences Utrecht and it determines the policy, measures and procedures in the field of Processing.

4.2 Personal data protection portfolio holder

The personal data protection portfolio holder is the board member with privacy in his portfolio. He bears ultimate responsibility for the protection of Personal Data at HU University of Applied Sciences Utrecht.

4.3 The data protection officer

HU University of Applied Sciences Utrecht has appointed an internal supervisor for the Processing of Personal Data. This supervisor is referred to as the data protection officer ("DPO"). HU University of Applied Sciences Utrecht will promptly involve the DPO in all matters relating to Personal Data. The statutory duties and powers of the DPO give this officer an independent position at HU University of Applied Sciences Utrecht. HU University of Applied Sciences Utrecht will register the DPO with the supervisory body.
The duties of the DPO are:

- to inform and advise all parties involved about their obligations under the GDPR;
- to monitor compliance with the GDPR and other relevant privacy legislation;
- to monitor compliance with this privacy policy by HU University of Applied Sciences Utrecht;
- to organise a Privacy Impact Assessment;
- to collaborate with the supervisory body;
- to act as the first point of contact for the supervisory body.

4.4 The application owner

The application owner is responsible for ensuring that the application and associated IT facilities offer good support to the process he is responsible for and he complies with the Policy. This means that the system owner ensures that the application complies and continues to comply with the requirements and wishes of users and with legislation, now and in the future.

4.5 The process owner

Creating awareness and compliance with the Policy form a part of the integrated management at the institutes, services and research centres. Every director and manager has the duty:

- to ensure that his employees are aware of the Policy;
- to monitor compliance of the Policy by his employees;
- to develop and manage appropriate working processes;
- to periodically raise the subject of privacy at work meetings.

5 The Implementation Policy

The Executive Board of HU University of Applied Sciences Utrecht is responsible for the Processing of Personal Data, the purpose and resources of which are determined by that board. It is deemed to be the **Controller** within the meaning of the GDPR. However, the actual Processing of Personal Data is undertaken at various levels at HU University of Applied Sciences Utrecht. The correct, efficient and responsible management of an organisation is often referred to with the term governance. It mainly also encompasses the relationship with the principal stakeholders of HU University of Applied Sciences Utrecht such as the owners, employees, students, other customers and society as a whole. A solid corporate governance policy looks after the interests of all Data Subjects.

5.1 The allocation of responsibilities

- The prudent processing of Personal Data should be seen as **a line responsibility**, i.e. the line managers (directors/managers of institutes, services and research centres) bear primary responsibility for the prudent Processing of Personal Data in their department/unit. This also encompasses the choice of measures and the implementation and enforcement thereof. Line responsibility also includes the duty to communicate the Personal Data Processing policy to all relevant parties.

- Handling Personal Data prudently is **everyone's responsibility**. Employees and students are expected to behave ethically. Intentional or unintentional behaviour that causes unsafe situations that, in their turn, result in damage and/or a loss of reputation of HU University of Applied Sciences Utrecht or individuals is not acceptable. For that reason, HU University of Applied Sciences Utrecht has formulated and implemented codes of conduct.

5.2 Incorporation into the university's governance/Coordination with adjoining policy areas

So as to clearly express the coherence in the organisation with regard to data protection and to coordinate the initiatives and activities in the field of the Processing of Personal Data at the various units, it is important to hold structured meetings about the subject of privacy at various levels.
On a **strategic level**, the parties talk specifically about governance and compliance, as well as about targets, scope and ambition in the field of privacy. The strategic level is structured at the administration department of HU University of Applied Sciences Utrecht, in consultation with the Executive Board.

On a **tactical level**, the strategy is translated into plans, standards to be applied and evaluation methods. These plans and tools control the implementation. The tactical level is structured by the directors per institute, service and research centre in the role of process owner.

On an **operational level**, the parties discuss the matters in relation to day-to-day management (implementation). The operational level is structured by privacy officers per institute, service and research centre.

5.3 Awareness and training

Policy and measures alone are not enough to exclude the risks of the processing of Personal Data. It is necessary to continuously raise awareness at HU University of Applied Sciences Utrecht so that knowledge of risks is improved and safe and responsible behaviour is encouraged. The regularly recurring awareness campaigns for employees, students and guests form a part of the Policy. These campaigns could tie in with national campaigns in higher education, possibly in coordination with other data protection campaigns. Raising awareness is the responsibility of the data protection officer.

5.4 Monitoring and compliance

The Policy can be monitored for effectiveness through audits. The DPO initiates the monitoring for the lawful and prudent processing of Personal Data.

Any external audits are carried out by independent auditors. This is linked to the annual audit and it is largely coordinated with the normal Planning & Control cycle.

In the event that compliance regarding the protection of personal data is seriously failing, HU University of Applied Sciences Utrecht can impose a sanction on the accountable employees in question within the frameworks of the collective agreement and the options offered by the law.

The processing of Personal Data is a continuous process. Technological and organisational developments at and beyond HU University of Applied Sciences Utrecht mean it is necessary to periodically check if the university is still on course with its Policy.

6 Lawful and prudent Processing of Personal Data

HU University of Applied Sciences Utrecht processes Personal Data in accordance with the principles set out in Paragraph 2.1 of this document. To elaborate these principles, HU University of Applied Sciences Utrecht has implemented the measures set out in this chapter.

6.1 Legal ground

HU University of Applied Sciences Utrecht only processes Personal Data if it concerns one of the legal grounds set out in Article 6 of the GDPR:

a) Consent of the Data Subject.
b) Is required for the implementation of an agreement with the Data Subject.
c) Is required in order to comply with a legal obligation of the controller.
d) Is required in order to protect the vital interests of the Data Subject or of another natural person.
e) Is required in order to fulfil a duty of a general interest or within the framework of exercising public authority.
f) Is required in order to look after the legitimate interests of the controller or a third party.

6.2 Privacy explanation

HU University of Applied Sciences Utrecht processes Personal Data in a way that is correct and transparent with regard to the Data Subject. This means that HU University of Applied Sciences Utrecht explains to the Data Subject to what extent and how his Personal Data is processed. When collecting Personal Data, HU University of Applied Sciences Utrecht will notify the Data Subject by means of a privacy explanation for each process/application. This notification is sent prior to the Processing of data unless this is, in all reasonableness, not possible. See also Paragraph 8.1 of this document.

6.3 Retention periods

Personal Data is not kept for any longer than is necessary for the purposes for which it is collected or used. After the expiry of the retention period6[5], Personal Data must be moved outside the scope of the active records. After the expiry of the retention period, HU University of Applied Sciences Utrecht will destroy the Personal Data or, if the Personal Data is intended for historic, statistical or scientific purposes, it will keep it in an archive.

6.4 Appropriate security measures

HU University of Applied Sciences Utrecht is responsible for an adequate level of protection and it must take the appropriate technical and organisational measures to protect the Personal Data from being lost and against any form of unlawful Processing. These measures also aim to prevent Personal Data from being collected and processed unlawfully.
A risk assessment of privacy protection and information security forms a part of the internal risk control and monitoring system of HU University of Applied Sciences Utrecht.

6.5 Obligation to document

HU University of Applied Sciences Utrecht has taken several measures in order to demonstrate it complies with the statutory requirements under the GDPR, including the implementation of this Policy. Furthermore, all fully or partially automated Processing of Personal Data has to be reported to the DPO of HU University of Applied Sciences Utrecht. The DPO assesses the validity of the Processing and he makes sure adequate documentation of all relevant data is available.
HU University of Applied Sciences Utrecht also conducts a Privacy Impact Assessment for (research) projects, infrastructural changes or the acquisition of new systems that are likely to pose a high risk for the rights and freedoms of natural persons. If this demonstrates that the Processing would result in a high risk in the absence of measures taken by HU University of Applied Sciences Utrecht to mitigate

[5] Retention periods may be stipulated by law as is the case with financial details or for more formal study results but they may also be stipulated by HU University of Applied Sciences Utrecht, for instance, in an agreement between HU University of Applied Sciences Utrecht and the Data Subjects.

the risk, HU University of Applied Sciences Utrecht will consult the supervisory body before it starts processing.

6.6 Privacy by Design and Privacy by Default

Every time it processes Personal Data, HU University of Applied Sciences Utrecht applies the principles of Privacy by Design and Privacy by Default.

6.7 Confidentiality

At HU University of Applied Sciences Utrecht, all Personal Data is regarded as confidential. Everyone has to be aware of the confidentiality of Personal Data and act accordingly.
Those not already subject to a duty of confidentiality by virtue of their jobs, professions or a legal stipulation, are also obliged to observe confidentiality with regard to the Personal Data they take cognizance of, unless any legal stipulation demands them to disclose the information or if their duties give rise to disclosing the information.

6.8 Special Personal Data

In principle, special Personal Data cannot be processed unless it concerns one of the statutory exceptions under the GDPR, which includes 'explicit consent of the Data Subject' and a 'substantial general interest', among other things. This special Personal Data is also subject to stricter protection requirements. When basic protection is insufficient, additional measures have to be taken that are coordinated for each individual information system.

Special Personal Data includes the following data:

- data that discloses race or an ethnic background;
- political convictions;
- religious or ideological convictions;
- data that discloses membership of a trade union;
- genetic details with a view to the unique identification of an individual;
- biometric details with a view to the unique identification of an individual;
- data concerning health;
- data with regard to an individual's sexual behaviour or sexual preferences.

Two types of Personal Data do not fall under the category of special Personal Data but the Processing and protection of that data *is* subject to strict requirements:

a) Personal Data with regard to convictions under criminal law and to crimes can be processed only under the supervision of the government or within European or national legislation.
b) Under Dutch legislation, a national identification number (the citizen service number [BSN] or the personal education number) can be processed only when this is stipulated by law.

6.9 The forwarding of Personal Data

6.9.1 Outsourcing Processing to a Processor

If HU University of Applied Sciences Utrecht outsources the Processing of Personal Data to a Processor, the implementation thereof is regulated in a processor's agreement between HU University of Applied Sciences Utrecht, the Controller, and this Processor.

6.9.2 The forwarding of Personal Data within the European Economic Area (EEA)

HU University of Applied Sciences Utrecht will only forward Personal Data to a Processor who is located within the EEA if the processing is based on one of the principles for data processing set out in Article 6 or Article 9 of the GDPR and if the Processor meets the statutory requirements set out in the GDPR.

6.9.3 The forwarding of Personal Data outside the EEA

HU University of Applied Sciences Utrecht will only forward Personal Data to Processors located in a country outside the EEA if one of the following conditions is met:

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

   For an appropriate level of protection, HU University of Applied Sciences Utrecht uses:
   - The general list of countries that offer an appropriate level of protection, published by the European Commission[6];
   - The Privacy Shield for businesses in the United States, published by the European Commission in cooperation with the US Department of Commerce[7].

2. Data is forwarded on the basis of the appropriate guarantees set out in Articles 46 and 47 of the GDPR.
3. Data is forwarded on the basis of the statutory exceptions set out in Article 49 of the GDPR.

6.10 Questions and complaints procedure

6.10.1 Reporting and registration

Questions or complaints about (the processing of) Personal Data can be submitted to the Privacy Desk. A log is kept of questions or complaints with a (potentially) significant impact. Questions and complaints can be reported by anyone, i.e. Data Subjects, Processors or Third Parties.

6.10.2 Security weak spots

Employees will log identified weak spots in systems or services and report them to the Privacy Desk immediately. A log is kept of all reports about security weak spots.

6.10.3 Processing

Questions, complaints and security weak spots are forwarded to the accountable department or person and are then processed in accordance with the specific procedures as soon as possible. If the Personal Data of a Data Subject or Data Subjects or the business processes, the finances or the reputation of HU University of Applied Sciences Utrecht are in serious danger, the DPO is notified, at least.

6.10.4 Evaluation

It is important to learn from the feedback given by means of the questions and complaints procedure. The logging of significant questions, complaints and weak spots and a period report about this form a part of the professional practice of processing Personal Data. That is why these reports form a fixed part of the annual report from the Executive Board and, if present, that of the DPO.

[6] You can find it on http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm.
[7] You can find it on https://www.privacyshield.gov/list.

7 Data breach

This chapter describes the policy with regard to the reporting, logging and processing of a Data Breach or a suspected Data Breach in the regular management and in special circumstances.

7.1 Data breach

A Data Breach is a breach of the security of Personal Data, resulting in any unauthorised Processing thereof. It may concern the theft of a laptop, a USB stick left on a train or an e-mail sent to the wrong person. Another example is giving someone unauthorised access to personal data in archives or digital systems such as Sharepoint. Data Breaches have to be reported to the supervisory body within 72 hours of discovery and, in some cases, also to the Data Subject.

7.2 Reporting and registration

At HU University of Applied Sciences Utrecht, a Data Breach may occur within the university's organisation but also at a Processor who is hired by HU University of Applied Sciences Utrecht. We distinguish the following situations:

a) *Employee*: if they discover a (suspected) Data Breach or if they fear they are themselves part of a Data Breach, employees have to contact the Privacy Desk via Askprivacy@hu.nl of HU University of Applied Sciences Utrecht.
b) *Processor:* a Data Breach may also occur at a Processor who is hired by HU University of Applied Sciences Utrecht. The Processor will report the Data Breach to HU University of Applied Sciences Utrecht in accordance with the processor's agreement that was concluded.
c) *Other persons:* if a person other than an employee or a Processor discovers a (suspected) Data Breach or if they fear they are themselves part of a Data Breach, they have to contact the Privacy Desk via Askprivacy@hu.nl.

A (suspected) Data Breach must be reported as soon as possible. The following details must be provided when reporting a Data Breach:

- Who reported the Data Breach?
- What has been reported?
- Where did the report originate from?
- What data does it concern?
- How did the incident occur?
- What systems are involved in/affected by the incident?
- When did the incident occur?
- If the Data Breach is reported by an employee of HU University of Applied Sciences Utrecht: what has been done in order to resolve the incident/prevent it from happening again?

Every Data Breach and the processing thereof is logged.

7.3 Processing

In the event of a Data Breach, it will be dealt with in accordance with the Data Breach provisions set out in the relevant legislation as described in the data breach reporting obligation policy of the Dutch Data Protection Authority[8] so that the Data Breach notification will reach the right persons in time and, ultimately, the supervisory body and the Data Subjects.
If the Personal Data of a Data Subject or Data Subjects or the business processes, the finances or reputation of HU University of Applied Sciences Utrecht are in serious danger, the DPO is notified, at least.

[8] Data breach reporting obligation policy of the Dutch Data Protection Authority: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf.

7.4 Decision-making

After a (suspected) Data Breach is reported in accordance with the previous paragraphs, the Privacy Desk will issue advice about the obligation to report the matter to the supervisory body and the Data Subject. The DPO will take this advice into consideration. The DPO will be responsible for the decision whether or not to report the matter.

7.5 Evaluation

It is important to learn from Data Breaches so as to reduce the probability of future Data Breaches. The registration of Data Breaches and periodic reports on the matter form a part of a professional way to process Personal Data. The report about Data Breaches in connection with Personal Data, therefore, forms a fixed element of the annual report from the Executive Board and the DPO.

8 Rights of the Data Subjects

The GDPR grants Data Subjects certain rights that enable them to control the Processing of their Personal Data.

The following applies to all rights of Data Subjects set out in this chapter:

- **Notification to the Data Subject**

HU University of Applied Sciences Utrecht ensures that the information and communications reach the Data Subject in a brief, accessible and comprehensible way and in a clear and simple language. The language will be geared to the target group.

- **Term**

A request from a Data Subject will be replied to as soon as possible but no later than four weeks after the request was submitted. The Data Subject will, in any case, be notified of the follow-up to his request. If the four-week term cannot, in all reasonableness, be met, the Data Subject will be notified within that term. In that case, HU University of Applied Sciences Utrecht will follow up the Data Subject's request within two months of the expiry of the first term.

- **The identity of the Data Subject**

When it provides the relevant information, HU University of Applied Sciences Utrecht ensures the identity of the person making the request is properly established. To that end, HU University of Applied Sciences Utrecht may ask for additional information.

- **Minors**

A request for a Data Subject - being a Minor, placed under guardianship or put under administration or a protection order - to exercise one of the rights set out in this chapter is made by his legal representative. Any reply from HU University of Applied Sciences Utrecht will be sent to this legal representative.

A written request to exercise the aforementioned rights can be sent to Askprivacy@hu.nl

8.1 The right to information

The Data Subject has the right to be notified by HU University of Applied Sciences Utrecht about certain aspects of the Processing of his Personal Data. HU University of Applied Sciences Utrecht notifies the Data Subject free of charge about the Processing of his Personal Data, both when the Personal Data is collected directly from the Data Subject and when it is obtained in a different way.

a) Obtained directly from the Data Subject

Prior to obtaining the data, HU University of Applied Sciences Utrecht will give the Data Subject the following information if the data is obtained directly from the Data Subject:

- The identity and the contact details of the Controller and, where applicable, the DPO.
- The specific purposes of the Processing for which the Personal Data is intended, as well as the legal ground for the processing.
- The legitimate interests of the Controller or Third Party when the Processing is based on the legal ground of 'legitimate interest'.
- When appropriate, the intention of the Controller to forward the Personal Data to a third country, the name of that country and how the Personal Data will be forwarded to that country.
- The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine those periods.
- The existence of the right to ask the Controller for access to, rectification or deletion of the Personal Data, a restriction of processing concerning the Data Subject, as well as the right to object to the Processing and the right to data portability.
- The right to lodge a complaint with a supervisory body.
- The recipients or categories of recipients of the Personal Data.
- If the Processing is based on the legal ground of 'consent', the Data Subject's right to withdraw that consent at any time.
- Whether the Personal Data is required for the implementation of an agreement or to fulfil a statutory obligation.
- Whether the Personal Data is also used for automated decision-making processes. The underlying logics, as well as the significance and anticipated consequences of the Processing for the Data Subject must also be reported.

b) Obtained indirectly from the Data Subject

If the Personal Data is not obtained directly from the Data Subject but via a different route, the Data Subject will receive the following information, in addition to the aforementioned points:

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

This information will be provided as soon as possible but no later than four weeks after obtaining the data or when contact is made with the Data Subject for the first time.

8.2 Right of inspection

- *Application*
  Every Data Subject has the right to ask if his Personal Data is processed and if that is the case, he has the right to inspect Personal Data that relates to him.

- *Notification*
  If data is processed, the notification from HU University of Applied Sciences Utrecht will contain a full overview of the following:
  - A description of the purposes of the Processing.
  - The categories of data which the Processing relates to.
  - Categories of recipients.
  - Information about the origin of the data.
  - The retention period of data or, if that is not possible, the criteria to determine that period.
  - The Data Subject's right to ask the Controller for rectification or deletion of data, restriction of or objection to Processing, as well as the right to data portability.
  - The Data Subject's right to lodge a complaint with a supervisory body.
  - All available information about the source of the data if the data was not obtained from the Data Subject.
  - Whether the Personal Data is also used for automated decision-making processes.
  - The underlying logics, as well as the significance and anticipated consequences of the Processing for the Data Subject must also be reported.
  - The appropriate safeguards that are in place when the data is forwarded to a third country.

Copy
The Data Subject can ask for a copy of all Personal Data. This copy must be issued in a customary electronic format unless the request was made on paper or if the Data Subject has explicitly asked for a paper copy.

- *Costs*

Every [first] copy is issued free of charge. HU University of Applied Sciences Utrecht may charge for additional copies, which will be discussed with the Data Subject first.

The rights and freedoms of others
When providing the data, HU University of Applied Sciences Utrecht will take the rights and freedoms of others into account.

8.3 The right to data portability

- *Reasons for a request*

Every Data Subject can submit a request to HU University of Applied Sciences Utrecht for a (free) copy of his data in a structured, customary and machine-readable format or to have it transferred directly to another Controller without experiencing any obstruction from HU University of Applied Sciences Utrecht if the following conditions are met:

1. The Processing of data by HU University of Applied Sciences Utrecht is based on the legal ground of 'consent' or that of 'implementation of an agreement with the Data Subject'.
2. The Processing in question is fully automated.

- *The rights and freedoms of others*

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

- *The removal of data*

If a Data Subject has exercised his right of data portability within the framework of data Processing to implement an agreement, HU University of Applied Sciences Utrecht cannot decide to delete the data. However, after the expiry of the retention period, HU University of Applied Sciences Utrecht will have to delete the data.

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

8.4 The right to rectification, supplementation, removal or restriction of Processing

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

Every Data Subject can ask to have his Personal Data held by HU University of Applied Sciences Utrecht corrected, supplemented or removed or to restrict the Processing thereof. In the case of the right to restriction, the Personal Data is temporarily blocked and is no longer processed by HU University of Applied Sciences Utrecht. The restriction is clearly mentioned in the file.

- *Notification*

If it emerges that the Data Subject's Personal Data held on record is, in effect, incorrect, if it is incomplete for the purpose or objects of Processing or if it is irrelevant or if it is otherwise processed in violation of a statutory regulation, the data manager (this can be both the functional manager and the Processor) will correct, permanently remove, supplement or restrict this data. Furthermore, Third Parties to whom the data was provided prior to the rectification, supplementation, removal or restriction will also be notified of this unless this is, in all reasonableness, not possible or, given the circumstances, irrelevant. The person making the request can ask for the name of the person to whom HU University of Applied Sciences Utrecht made this notification.

- *Implementation term*

The data manager ensures that a decision to correct, supplement, remove or block data is implemented as soon as possible. This implementation is free of charge for the Data Subject.

8.5 The right to object

- *Grounds for objection*

Data Subjects can object to the Processing of data for two reasons:

1. For reasons of personal circumstances, every Data Subject can object to the Processing of data by HU University of Applied Sciences Utrecht if this Processing takes place on the basis of a) the fulfilment of a duty of a general interest or within the framework of exercising public authority by the Controller, or b) looking after the legitimate interests of HU University of Applied Sciences Utrecht or a Third Party to whom the data is provided. For a description of the legal grounds, see Paragraph 6.1.

   In principle, HU University of Applied Sciences Utrecht will stop the Processing of data when it receives an objection. If HU University of Applied Sciences Utrecht can prove that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the Data Subject, the Processing of data will resume. If the objection is legitimate, HU University of Applied Sciences Utrecht will take measures (free of charge) required in order to no longer process the Personal Data for the purposes in question.
2. When data is processed for the purpose of 'direct marketing', a Data Subject will at all times have the right to object. In the case of an objection to the Processing of data for direct marketing purposes, HU University of Applied Sciences Utrecht will stop and continue to stop the process immediately (free of charge).

8.6 Automated decision-making

Grounds

Data Subjects have the right not to be subjected to a decision that is based exclusively on automated Processing and which has legal consequences for him. A 'decision based on automated Processing' refers to a decision that is made without any human intervention. Among other things, this includes Profiling.

HU University of Applied Sciences Utrecht can take decisions based on automated Processing in the following three situations only:

1. If the decision is required in order to conclude or implement an agreement with the Data Subject.
2. If the decision is allowed under a European or national law, provided this law provides for appropriate measures to protect the rights and freedoms and legitimate interests of the Data Subject.
3. If the decision is based on the explicit consent of the Data Subject. This consent can be withdrawn at all times.

In all of the aforementioned situations, HU University of Applied Sciences Utrecht will take appropriate measures to protect the rights and freedoms and legitimate interests of the Data Subject. This will, in any case, include the right to human intervention by HU University of Applied Sciences Utrecht, the Data Subject's right to voice his opinion, as well as the right to object to the decision. Minors will never be subjected to automated decision-making.

8.7 Legal protection

- *General complaints*

If the Data Subject is of the opinion that the statutory provisions with regard to privacy protection or the provisions of these regulations are not enforced correctly towards him, he can submit a written complaint to the Data Protection Officer of HU University of Applied Sciences Utrecht via roos.roodnat@hu.nl

- *Other objection options*

Apart from the general internal complaints procedure set out above, the Data Subject has the following options if he feels that HU University of Applied Sciences Utrecht has violated the GDPR to his disadvantage:

A. Application proceedings at the sub-district court

If HU University of Applied Sciences Utrecht has issued a negative decision with regard to a request as set out in Paragraphs 8.1 to 8.6 of this document or if HU University of Applied Sciences Utrecht has denied the Data Subject's request, the Data Subject can start application proceedings at the sub-district court.

The application must be submitted to the sub-district court within six weeks of receiving the reply from HU University of Applied Sciences Utrecht. If HU University of Applied Sciences Utrecht fails to reply to the Data Subject's request within the term given, the application must be submitted within six weeks of the expiry of that term. The application does not have to be submitted by a lawyer.

B. Enforcement request to a supervisory body

If HU University of Applied Sciences Utrecht has issued a negative decision with regard to a request as set out in Paragraphs 8.1 to 8.6 of this document or if HU University of Applied Sciences Utrecht has denied the Data Subject's request, the Data Subject can submit a complaint to a supervisory body or ask an interest group to act on his behalf.

9 A final note

This document was adopted by the Executive Board of HU University of Applied Sciences Utrecht on 22 May 2018 subject to consent of the Employees' and Students' Council.
A policy review forms a part of the half-yearly plan-do-check-act cycle of HU University of Applied Sciences Utrecht. This also includes a check on the effectiveness of the measures.

The most recent version is published on www.hu.nl/privacy

If you have any questions or comments with regard to this policy, please contact the Privacy Desk via Askprivacy@hu.nl