HU University of Applied Sciences Utrecht Privacy Policy

Author
Privacy manager
IM&ICT Service

Date
4 July 2024

Version
3.2.1

Version management

Version	Date	Author	Processing
1.0	15 May 2018	Roos Roodnat	Publication on HU.nl
2.0	March 2022	Rinske Plomp	Privacy policy update
2.1	25 July 2022	Rinske Plomp (review Eric van den Bos, Annelies de Jeu, Roos Roodnat)	Adjusted privacy policy structure after review : in line with IBB structure and format
2.2	24 March 2023	Rinske Plomp	Update to changes in policy after July 2022
3.0	17 Aug 2023	Rinske Plomp (review Roos Roodnat, Marcel van de Kolk, Rene Anker)	Update following amended Information Security Policy
3.1	14 April 2024	Rinske Plomp (review Roos Roodnat, Han Wouters, Eelko van Leeuwen)	Update following new developments
3.2	12 June 2024	Roos Roodnat	Discussion points EB meeting implemented
3.2.1	4 July 2024	Roos Roodnat	Discussion points EB/HSR implemented

Distribution list

Version	Date	Recipient	Objective
3.0	29 Aug 2023	EB	Forwarding
3.1	11 June 2024	EB	Forwarding
3.2	3 July 2024	HSR	Consent
3.2.1	9 July 2024	EB	Adoption

Content

1 Introduction

HU University of Applied Sciences Utrecht is a knowledge institute. Education, research and professional practice are the most important processes in a university of applied sciences. Storage and processing of personal data is necessary for education and conducting research. For students, staff members and others involved with HU University of Applied Sciences Utrecht, it is important that this is done with the utmost care. HU University of Applied Sciences Utrecht is therefore committed to protecting the personal data provided to it. It is the responsibility of every staff member and student to handle this carefully and comply with privacy legislation (General Data Protection Regulation, GDPR). Behaviour and privacy expertise largely determine how securely we handle personal data.

Together with companies and institutions, our students, lecturers, researchers, staff members, management, participatory decision-making and board work to professionalise and innovate professional practice. The boundaries between institutions are less and less important in this respect. This means we will have to further develop ourselves into an open network organisation. This also poses safety risks. We simultaneously have a social obligation and moral and legal responsibility to provide a safe learning and working environment for all involved. In that area of tension, we think a thoughtful approach to integrated safety is important.

Integrated safety in the HU means that we address safety-related issues within the institution in a coherent way and that we reason from the same strategic framework for all domains in the field of integrated safety. This vision gives us direction in the choices we make regarding the different areas of integrated safety at tactical and operational level.

The HU distinguishes several safety domains: Information safety, social safety, physical safety and crisis management. Personal data protection, together with information safety and knowledge safety, falls under the information safety domain. The IM&ICT director bears HU-wide responsibility for the information safety domain.

1.1 Purpose of privacy policy

HU University of Applied Sciences Utrecht's privacy policy aims to optimise the quality of processing and security of personal data. This must strike a good balance between privacy, functionality and safety. The frameworks and tools in the policy give HU University of Applied Sciences Utrecht insight into its working methods and thus also raise awareness of the importance and necessity of protecting personal data, among staff members and students.

By describing the measures in this Privacy Policy, HU University of Applied Sciences Utrecht takes responsibility for optimising the quality of processing and security of personal data and thus complying with the relevant privacy laws and regulations (the GDPR and the GDPR Implementation Act).

Policy instruments and policies are only the beginning. To make privacy part of our day-to-day operations, there is a strong privacy organisation, with each institute, research centre and service having its own privacy officer. Colleagues can come to them with questions and advice. Most importantly, both staff members and students are aware that they are working with personal data and know how to do so carefully. This requires constant attention.

This privacy policy is an update of the privacy policy adopted in May 2018, i.e. when the GDPR came into force. In this privacy policy, the processes were further updated, and the design of the privacy organisation was renewed.

More specific objectives of the privacy policy are:

- Meeting legal requirements and accountability (DPIA, Processing Register, Processor Agreements)
- Providing support and advice for data subjects to exercise their rights (e.g. request for inspection).
- Providing concrete guidelines and formats for both education and research practice to handle personal data with care (elaborated at the operational level).
- Raising awareness among all staff members and students
- Properly handling reports of a data breach

1.2 Scope of privacy policy

1.2.1 HU University of Applied Sciences Utrecht Privacy Policy

The privacy policy relates to the processing of personal data of all data subjects which in any case includes all staff members, students, guests, alumni, student voters, visitors, respondents and external relations (hiring/outsourcing).

For HU University of Applied Sciences Utrecht, personal data protection is part of Integrated Safety and always relates to all safety domains: information safety, social safety, building safety integrity and physical safety and crisis management. The safety organisation pays constant attention to these interfaces and seeks coordination both in terms of plan and content.

1.2.2 Third parties

The HU has contracts with other organisations in the form of partnerships, participations, resource sharing, etc. Based on risk analysis, the information security requirements that parties need to meet to enable secure exchange and/or processing of data are determined prior to cooperation. These requirements will be included in a programme of requirements. The arrangements must then have to be explicitly set out in the contract, and compliance with these arrangements must be reviewed periodically.

Where HU University of Applied Sciences Utrecht has personal data processed by an external processor, the performance of processing operations will be governed by a processor's agreement. This processing agreement is part of the contract the HU enters into with the supplier or cooperation partner. If there is joint responsibility for processing, this is also set out in an agreement. The HU uses the formats established jointly with SURF.

The processor agreements are recorded in the central processing register. Monitoring and auditing of the agreements set out in the processor agreement also takes place from this register.

The HU University of Applied Sciences Utrecht only discloses personal data to a Processor located *within* the EEA if the processing is based on one of the data processing grounds in article 6 or article 9 of the GDPR and if the Processor complies with the legal requirements under the GDPR:

HU University of Applied Sciences Utrecht only provides personal data to Processors located in a country *outside* the EEA if the third country, territory, well-defined sector in a third country, or the international organisation in question offers an adequate level of protection according to the European Commission.

As an appropriate level of protection, HU University of Applied Sciences Utrecht applies:

- The general list of adequacy countries published by the European Commission[1].
- The Standard Contractual Clause (SCC) for companies previously covered by the Privacy Shield. The SCC is modular and can be applied in different roles and therefore also between joint processors. Transfers are made on the basis of appropriate safeguards from the GDPR, articles 46 and 47.
- Transfer takes place on the basis of one of the legal exceptions in article 49 of the GDPR.

1.3 Collaboration

The GDPR is relatively young legislation. This requires standard setting, knowledge development and continuous honing of processes based on case histories. The Privacy Organisation therefore chooses to work and coordinate closely with the Education sector. To this end, it actively participates in the following networks:

- SURF: SCIPR community
- IVHO: Integral Safety Consultation Higher Education (Integraal Veiligheidsoverleg Hoger Onderwijs)
- Data Protection Officer (Functionaris Gegevensbescherming, FG) network Netherlands Association of Universities of Applied Sciences
- Network GDPR and Education
- Network Privacy Managers Universities of Applied Sciences

The formats and guidelines developed by these networks for education are important starting points for implementations within the HU.

2 Principles and Policy Principles

2.1 Policy principles

General policy principle is that personal data are processed in accordance with relevant laws and regulations in a proper and careful manner. HU University of Applied Sciences Utrecht adheres to the elaboration of the GDPR and related legislation such as the GDPR Implementation Act and Dutch Archive Act [Archiefwet].

Legitimate

HU University of Applied Sciences Utrecht only processes personal data if one of the bases described in Article 6 of the GDPR applies:

a) Consent of data subject.
b) Necessary for the performance of a contract with the data subject.
c) Necessary to comply with a statutory compulsory obligation incumbent on the controller.
d) Necessary to protect the vital interests of the data subject or another natural person.

[1] These can be found via the following link http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm.

e) Necessary for the performance of a task in the public interest or in the exercise of public authority.
f) Necessary to pursue the legitimate interest of the processing controller or a third party.

Purpose limitation
When processing, a proper balance must be struck between HU University of Applied Sciences Utrecht's interest in processing personal data and the interest of the data subject. The latter to respect his privacy and to freely make his own choices regarding his personal data.

Special personal data
Processing of special personal data is in principle prohibited, unless one of the statutory exceptions in the GDPR applies, which include 'explicit consent of the data subject' and a 'substantial public interest', or a specific provision in the GDPR Implementation Act. This provision applies, for example, when providing care and guidance and planning if students' health conditions require it.

More stringent requirements also apply to the security of this special personal data. Where basic protection is not sufficient, individually tailored additional measures must be taken for each information system.

Special personal data includes the following data:
- data revealing racial or ethnic origin;
- political views;
- religious or philosophical beliefs;
- data showing union membership;
- genetic data for the purpose of uniquely identifying an individual;
- biometric data for the purpose of uniquely identifying an individual;
- data on health;
- data relating to a person's sexual behaviour or sexual orientation.

Two types of personal data do not fall under the category of special personal data, but their processing and security are subject to strict requirements:
- Processing of personal data relating to criminal convictions and offences may only be carried out under government supervision or within European or national legislation.
- Under Dutch law, a national identification number (the citizen service number or education number) may only be processed if it is provided for by law.

Data minimalisation
Only those personal data necessary for our tasks are processed. Also, only people who need the data to perform their duties must have access to the data.

Retention periods
Personal data will not be kept longer than necessary for the purposes for which it was collected or used. HU University of Applied Sciences Utrecht will destroy the personal data after the expiry of the retention period or, if the personal data are intended for historical, statistical or scientific purposes, keep them in an archive. Retention periods may be stipulated by law, such as for financial data or formal study results. The Higher Education Selection List serves as the starting point for this. Retention periods may also be laid down in a processing agreement or in an agreement between HU University of Applied Sciences Utrecht and the data subjects.

Secure and reliable (Privacy by design)
Personal data is adequately secured according to the applicable security standards (availability, integrity and confidentiality). When processing personal data in projects and systems, the principle of privacy by design is applied. No more personal data is processed than necessary and access is limited

to those who have rights to it.

Transparent
The HU complies with the obligations under the GDPR when it comes to accountability and transparency, such as maintaining processing records, preparing privacy statements and exercising data subjects' rights. All information can be found on the Knowing&Regulating (Weten&Regelen) page, Privacy and Security on ONE HU and for external parties on the HU/privacy website.

Data subjects' rights
Processing personal data requires the consent of the data subject in a number of situations. This is the case where there is no statutory duty or legitimate interest. Important conditions for consent are that the data subject is well informed, gives voluntary consent and knows his/her rights. For example, one of his rights is that he can withdraw consent.

The Privacy Act (GDPR) gives all people whose personal data is processed specific rights. Everyone has the right to see the personal data HU University of Applied Sciences Utrecht collects from him or her; to amend it if it is incorrect or incomplete. In specific situations, data subjects can also have data deleted or processing restricted (stopped). People wishing to exercise these rights can contact the privacy desk of HU University of Applied Sciences Utrecht (via Askprivacy@hu.nl). These rights are further detailed in sections 2.3.8 and 2.3.9.

Appendix 1 explains GDPR terms in more detail.

2.2 Laws and regulations observed

HU University of Applied Sciences Utrecht implements its privacy policy based on legal frameworks such as the (U)GDPR, of course, but also the Higher Education and Research Act [Wet op het Hoger onderwijs en Wetenschappelijk onderzoek, WHW] and the Archives Act. Important guidelines to flesh out this policy are the Higher Education Selection List in terms of data retention. In addition, ISO and SURF provide guidelines for further sharpening and concretisation of the policy.

Relevant legislation and directives

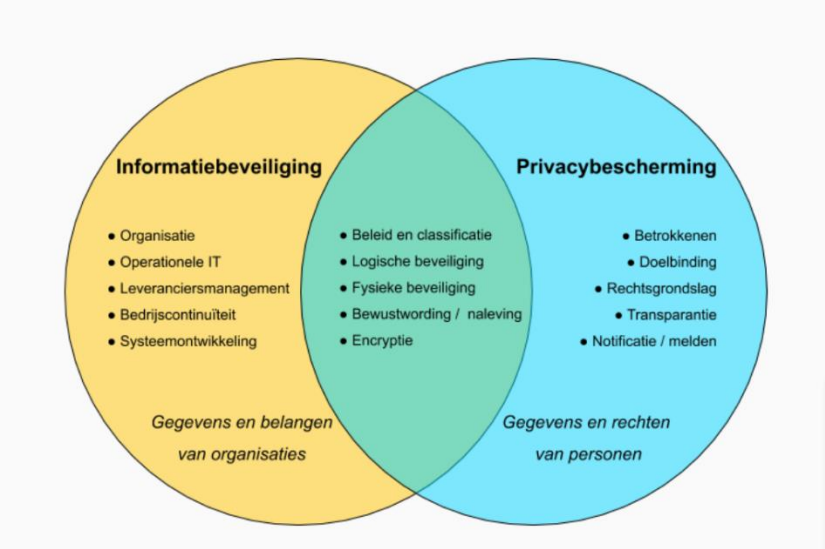
The main laws and regulations applicable to the HU with an impact on privacy and information security policies are:

- General Data Protection Regulation (GDPR)
- General Data Protection Regulation Implementation Act (GDPR Implementation Act)
- Higher Education Selection List
- SURF privacy audit (maturity levels per cluster of obligations)
- AI EC regulation
- Published recommendations/guidelines Personal Data Authority
- Published recommendations/guidelines SURF
- Medical Treatment Agreement Act [Wet op de geneeskundige behandelovereenkomst, WGBO]/Individual Health Care Professions Act [Wet op de beroepen in de individuele gezondheidszorg, Wet BIG]/Health Care Client Rights Act [Wet cliëntenrechten zorg, Wcz]
- Higher Education and Research Act (WHW)
- Public Records Act [Archiefwet]
- Copyright Act [Auteurswet]

Appendix 2 details the relevant laws and regulations.

2.3 GDPR Principles

Protection of personal data is conditional on the information systems in which it is processed being properly secured. Therefore, there is also overlap in the principles of both information security and privacy. The figure below clarifies the differences as well as the common ground.



Source: what do privacy and information security have to do with each other? - Axxemble

The information security policy (HU University of Applied Sciences Utrecht, 2019) elaborates on these principles, including implications and responsibilities. The key principles in this information security policy, which are also highly relevant to privacy protection, are:

- Information security is risk based
- Security by Design
- Security by Default
- Data has one owner
- Information access is role based

This section of the privacy policy specifically addresses the principles that primarily affect the protection of personal data.

2.3.1 The university of applied sciences informs data subjects about the processing of personal data

Rational	The HU must inform everyone whose personal data are processed what personal data are processed, on what basis and how these data are protected. This is explained in the privacy statement. The HU has privacy statements for various stakeholders, such as our students, staff members, alumni and students. For major projects where (new) personal data are processed, a privacy statement is drafted for specifically that purpose. The privacy statements are published on Knowing& Regulating on EEN HU (One HU) and on the regulations site and are actively brought to the attention of new staff members and trainees.

Implications	• Data owners, project leaders must assess at the initiative phase whether a privacy statement is necessary. • To this end, they can seek advice from their privacy officer or the privacy manager • The privacy officer or manager prepares a draft privacy statement using a set format. • The FG advises on the draft text. • Privacy statements must be published in an accessible way, and data subjects must be made aware of them, for example when requesting consent.
Accountable	• EB
Responsible	• HU director
Consulted	• Privacy officer, Privacy manager, FG
Informed	• Project management

2.3.2 HU University of Applied Sciences Utrecht maintains a processing register

Rational	Every organisation is required to keep a register recording all processing operations involving personal data. This therefore applies to all HU processes that process personal data, even if they do not require a processor agreement. The register must be delivered at the request of the Personal Data Authority. The register is not only an accountability tool but also provides access to the processing operations in the event of a data breach or an inspection request. It is also the central register for the processor agreements entered into. You can find information on the processing register on EEN HU.
Implications	• Organisational units (data owners) are themselves responsible for keeping track of their processing operations. • The administrator of the processing register supports the privacy officers and, together with the privacy manager, monitors the completeness and quality of the register. • In the register, we try to match the terminology of the HU processes as much as possible. • The FG assesses the legality of processing operations.
Accountable	• EB
Responsible	• HU director
Consulted	• Privacy officer, Privacy manager, FG
Informed	• Process or system owners of a process, project leaders

2.3.3 Privacy by Design

Rational	Privacy by design means taking into account the security and protection of (personal) data already during the start of a project, the design of a new application or ICT environment. This is a legal requirement under the GDPR, but also prevents remedial action afterwards.
Implications	• The business process owner is responsible for ensuring that security requirements (non-functional requirements) are included in every new project/IT system/innovation from the start. • Through a (pre)DPIA, risks to the protection of personal data are detected and mitigating measures are named.

	• The FG advises on the DPIA carried out and the measures to be taken. In the case of a serious personal data breach, the FG submits the opinion to the Personal Data Authority. • Before going live, the application of the security requirements will be reviewed and/or tested by or on behalf of Team Strategy & Compliance of the IM&ICT Service. • The principle of 'least duty' is applied. This means striving to grant no more rights than are necessary for adequate function and business operations • Where applicable, personal data will be anonymised. • No personal data from the production environment are used in test and acceptance environments. • The business process owner applies information security risk assessment and the principles of administrative organisation (AO) when setting up task responsibilities and authorities.
Accountable	• Business Process Owner
Responsible	• Business Process Owner
Consulted	• Privacy officer, FG • Business Control Service • Processing Team, IM&ICT Service • Strategy & Compliance Team, IM&ICT Service
Informed	• Functional administrator, Technical administrator

2.3.4 Privacy by Default

Rational	Privacy by Default means that in every configuration implemented for security options present, the most secure option is activated. This is a legal obligation under the GDPR and prevents unwanted and uncontrolled access to (personal) data.
Implications	• The baseline of the default configuration must be defined. • The principle in initial design of an information system is "closed unless.... • "Deviation from the initial set-up must follow the 'comply or explain' principle." • Control of this is secured in the change management process.
Accountable	• Owner of a technical component (service, application, server, network component etc.)
Responsible	• Owner of a technical component (service, application, server, network component etc.)
Consulted	• Strategy & Compliance Team, IM&ICT Service
Informed	• Functional administrator, Technical administrator

2.3.5 The HU has a low threshold data breach procedure in place

Rational	A data breach occurs when there is a personal data security breach that results in unauthorised processing. Data breaches must be reported within **72** hours of discovery to the Personal Data Authority and, in some cases, also to the data subject (see also Chapter 5).

	A Data Breach may occur within the organisation itself, but also at a processor engaged by the HU University of Applied Sciences Utrecht. A data breach must be reported internally as soon as possible via the notification form. If a reporter wishes to remain anonymous, it is also possible to contact the FG by phone. EEN HU explains what a data breach is and why it is important to always report (a suspected) data breach.
Implications	• Staff members must, if they observe a (possible) data breach or believe themselves to be part of a data breach, make a notification by filling in the notification form found on EEN HU and on HU Wegwijs (HU Wayfarer). This form will automatically reach the privacy desk and the FG's mailbox. • It is also possible that a data breach may occur at a processor engaged by HU University of Applied Sciences Utrecht. In accordance with the concluded processing agreement, the processor will report the Data Breach to the FG of HU University of Applied Sciences Utrecht. • Other stakeholders can send an email directly to the FG. Contact details are listed on the HU website under privacy. • When reporting a data breach, the following information is at least included: o Who reported the data breach? o What has been reported? o Where did the reporting come from? o What data is involved? o How many data subjects were (potentially) leaked? o How did the incident take place? o Which systems were involved/affected by the incident? o When did the incident take place? • Depending on the cause of the data breach and the impact, an investigation team is put together. If security measures need to be taken immediately, they work closely with security colleagues (CERT) or take the lead in the investigation. • If it concerns a very high-impact data breach, it is scaled up to a crisis team and the EB and spokesperson are also involved. • The FG and the director of the relevant organisational unit are kept informed and involved in decision-making. If it is a security issue, the IM&ICT director will also be involved in further handling. • If the data breach affects data subjects, they will be informed. • All data breaches are recorded in a register. The FG makes an annual report of data breaches and their cause. This also contains an interpretation and advice on measures to be taken to prevent a data breach as much as possible. The privacy officers bring this report and advice to the attention of their own MT. • To encourage reporting and make staff members and students feel free to report a data breach, communication with the reporter will always be constructive. • Staff members can always report a data breach on their own initiative, no consultation or permission from a supervisor is necessary. • The deliberate failure to report a data breach with major consequences for the organisation (deliberate failure to act, dereliction of duty) may lead to measures towards the staff members as included in CAO article P3.
Accountable	• EB
Responsible	• Director/Data owner (in the HU practice: business process owner)
Consulted	• FG, Privacy manager, Privacy officer, Information Security officer, JZ, spokesperson

Informed	• Staff members involved in the data breach (the system/process where the data breach occurred). • Notifier • Data subjects if the data breach poses risks to their personal data.

2.3.6 A DPIA is carried out for new processing operations and systems

Rational	The HU University of Applied Sciences Utrecht carries out a Data Protection Impact Assessment (DPIA), in the case of (research) projects, infrastructural changes or the acquisition of new systems that are likely to pose a high risk to the rights and freedoms of individuals. In some cases, existing projects and systems are also evaluated through a DPIA. After three years, a DPIA is repeated, and any new risks and changes are identified. SURF carries out Vendor Compliance DPIAs on systems used by many educational institutions. Where SURF conducts a DPIA, the HU adopts the findings and determines the measures necessary for the HU. Where AI applications are concerned, jointly with other expertise within the HU (think ethics, digitalisation) a Human Rights and Algorithm Impact Assessment (Impact Assessment Mensenrechten en Algoritme, IAMA) or a question set from the IAMA will also be involved in the assessment.
Implications	• The privacy officer will use a Pre-DPIA to assess whether a DPIA is necessary. If necessary, he/she will seek advice from the privacy manager. • The FG advises the data owner to carry out a DPIA. • The privacy officer organises the DPIA for their own projects, always on behalf of the data owner. • The privacy manager is responsible for carrying out the DPIA when it comes to HU-wide projects and advises the privacy officers in their DPIA. • The DPIA involves the various stakeholders (project management, security, functional management, stakeholder). • Expansion to an IAMA will also involve the relevant expertise. • The FG then advises on action to be taken based on the report. • If it appears that a processing operation constitutes a high risk and if the HU University of Applied Sciences Utrecht is unable to take the desired measures, the FG will consult the supervisory authority prior to the processing. • HU uses the central government DPIA format and has established a procedure for its own organisation.
Accountable	• EB
Responsible	• HU director
Consulted	• Privacy officer • FG • Stakeholders participating in the DPIA (security, stakeholders, functional management)
Informed	• Colleagues involved in the system/process

2.3.7 Privacy legislation explained in unambiguous and easy-to-find instructions

Rational	Everyone needs to be aware of the value of information and privacy of data subjects and act accordingly. This value is determined by the potential damage due to loss of availability, integrity or confidentiality. Staff members, students and third parties alike are expected to handle information consciously and contribute to the security of the automated systems and the (personal) data stored in them. Because knowledge of both privacy and information security are prerequisites, awareness activities are always taken up jointly on the basis of both disciplines. For case histories, staff members and students can contact their privacy officer. If desired, the question can also be submitted to the privacy desk or the privacy manager. Requests for advice can range from case histories such as may I ask the reason for sickness absence, to requests for advice on projects and new systems.
Implications	• Awareness of risks, HU security procedures and the handling of personal data are addressed when new staff members and students join. Among others, through the brochure for new staff members and the introduction programme at EEN HU. • For all users of the HU information facilities, *ICT Rules of Conduct and a code of conduct on handling data* are available via EEN HU. This code applies to students, staff members and third parties alike. • There is a privacy consideration framework that goes through some of the key rules of thumb of the GDPR, supporting in giving advice. • On EEN HU, all important instructions are on Knowing&Regulating/Privacy and Security. An e-learning course on Privacy is available in myTalent (mijnTalent) for permanent staff members. • Staff members and third parties sign for safe handling of information and data carriers. • The HU regularly organises cybersecurity and privacy awareness activities for its various target groups: students, staff members, managers and partners of the HU. • Current developments and publications are highlighted via a privacy newsletter and blogs on EEN HU Information Security. • Violation of information security laws, regulations and rules may lead to sanctioning measures, by or on behalf of the Executive Board.
Accountable	• EB
Responsible	• HU Director, Privacy manager
Consulted	• Privacy officers, Information Security Officer, JZ
Informed	• All staff members, students and partners of the HU

2.3.8 Data subjects can exercise their privacy rights

Rational	Permission Processing personal data requires the consent of the data subject in a number of situations. This is the case where there is no statutory duty or legitimate interest. This might include interviewing respondents or filming a treatment for a practical lesson. Permission is also required when using videos or photos to add to a message in a newsletter or on a website. Important conditions for consent are that the data subject is well informed, gives voluntary consent and knows his/her rights. For example, one of his rights is that he can withdraw consent.

	Data subjects' rights
	
	The Privacy Act (GDPR) gives all people whose personal data is processed specific rights. Everyone has the right to access the personal data HU University of Applied Sciences Utrecht collects from them;
	
	• to review;
	• to change the personal data if it is incorrect or incomplete;
	• to have them deleted in the following cases:
	  ○ if the data are no longer needed for the purpose for which they were collected;
	  ○ if a given consent is withdrawn and this consent is the only basis on which the collection is based;
	  ○ if the personal data have been collected unlawfully;
	• to restrict (stop the processing of personal data). The data may then only be processed in the following cases:
	  ○ with permission;
	  ○ for establishing, exercising or substantiating a legal regulation;
	  ○ to protect the rights of others.
	A request to exercise the above rights may be made in writing askprivacy@hu.nl.

Implications	• The HU University of Applied Sciences Utrecht ensures that information and communication about these rights is provided to data subjects in a concise, accessible and understandable manner. • A request (e.g. inspection) from a data subject shall be responded to in writing as soon as possible, but no later than one month after submission. In doing so, the data subject will in any case be informed of the action taken on the request. • If the one-month period is not reasonably practicable, the person concerned will be notified within this period. In this case, the HU University of Applied Sciences Utrecht will act on the data subject's request within two months of the expiry of the first term. • When providing the relevant information, the HU University of Applied Sciences Utrecht will ensure that the identity of the applicant is properly established. To this end, the HU University of Applied Sciences Utrecht may request additional information. • A request for the exercise of any of the rights by a minor, a data subject who is under guardianship or for whose benefit a guardianship or mentorship has been established must be submitted by his/her legal representative. A response by the HU University of Applied Sciences Utrecht will also be sent to this legal representative. • The data subject may request a copy of all personal data. This copy must be provided in a commonly used electronic format, unless the data subject explicitly requests a paper copy. Any (first) copy can be requested free of charge. • The HU University of Applied Sciences Utrecht will take into account the rights and freedoms of others when providing data. • Personal data whose retention period has already expired but which the HU still holds must also be provided. • These rights also apply to personal data stored in non-official documents, such as an email message or a report.
Accountable	• EB

Responsible	• HU Directors
Consulted	• FG, Privacy manager, Privacy officer, JZ, IM&ICT in case of searches
Informed	• All staff members, students and partners of the HU

2.3.9 Complaints and appeals procedure

Rational	In addition to the rights described in 2.3.8, the data subject has the following options if he or she believes that the HU University of Applied Sciences Utrecht has not complied, or has not sufficiently complied, with the GDPR. *Application procedure in the subdistrict court* If HU University of Applied Sciences Utrecht has made a negative decision on a request as described in the exercise of rights, or has rejected the data subject's request, the data subject may initiate petition proceedings with the subdistrict court. *Application for enforcement to supervisory authority* If HU University of Applied Sciences Utrecht has rejected a request as described at 2.3.8, or HU University of Applied Sciences Utrecht has rejected the data subject's request, the data subject has the option of filing a complaint with a supervisory authority or having an interest group act on their behalf.
Implications	• The petition must be submitted to the subdistrict court within six weeks of receiving the reply from the HU University of Applied Sciences Utrecht. • If the HU University of Applied Sciences Utrecht has not responded to the request of the party concerned within the set time limit, the petition must be filed within six weeks of the end of that time limit. Submission of the petition need not be done by an attorney-at-law.
Accountable	• EB
Responsible	• HU director
Consulted	• Privacy manager, Privacy officer, FG, Legal Affairs (Juridische Zaken, JZ)
Informed	• All staff members, students and partners of the HU

2.3.10 All IT facilities are commissioned through the standard change process

Rational	With the continued digitisation of both education and research, as well as home working and online collaboration, there is a need for continuous innovation. Using new tools and apps is a logical step in this regard. However, the tools may process personal data of lecturers and students, pass it on to third parties or set cookies. Just by logging in with the HU account, data is shared from the HU profile. It is therefore not allowed to use unapproved apps, even (especially) if they are free.
Implications	• Colleagues wishing to acquire a new app must do so within the appropriate privacy and security frameworks. They have to fill an Application Form for this purpose. • The application is assessed by the Business IT consultant at IM&ICT on added value, availability of similar apps, functionality in application landscape and management. In consultation with colleagues from privacy and security, we assess whether the supplier meets the appropriate requirements. • With the aforementioned colleagues, a procedure for requesting applications has been established and published on EEN HU. • A processor agreement must be drawn up with the relevant supplier.

	• In those cases where there are deviations from the HU guidelines, the comply-or-explain register must be completed. The director concerned is thus responsible for the risks arising from the deviation. • An overview of authorised and approved applications will be made available.
Accountable	• EB
Responsible	• HU director
Consulted	• BIT consultant, information security officer, privacy manager • Procurement consultants • Privacy officer • FG
Informed	• Staff members of the HU

2.3.11 Privacy protection is an ongoing process

Rational	The environment is constantly changing; cyber threats increase and decrease; processes change, staff members and students change, etc. New projects and forms of processing are emerging. Only defining and implementing measures once is insufficient to maintain a safe climate. Information security and privacy policies only make sense if this is a continuous process of taking measures, awareness and controls. The HU University of Applied Sciences Utrecht works on the basis of a risk-oriented approach for all security domains. Within the Information Safety domain, for privacy, information security and knowledge safety, risks have been defined, estimated and mitigating measures formulated. These measures are included in the Annual Information Safety Plan. Risks have been determined for the areas of Compliance (applying SURF's standards framework), Governance, Awareness and Incident handling. We also conduct a number of standard reviews and evaluations.
Implications	• Review procedures and guidelines regularly (at least 2 annually). • Privacy procedures and policy documents are subject to a PDCA cycle • Audits (including the SURF standards framework) and assessments make it possible to check the policy and measures taken for effectiveness (verifiability) and identify opportunities for improvement • Privacy policies are periodically reviewed by the FG through assessments and within existing privacy consultations. Improvement measures are then initiated by the privacy organisation. • FG reports key current developments, findings and signals in quarterly and annual reports • Improvements to measures, procedures and policies are implemented systematically
Accountable	• EB
Responsible	• HU Director, Privacy manager
Consulted	• FG
Informed	• Privacy officer

3 Privacy organisation

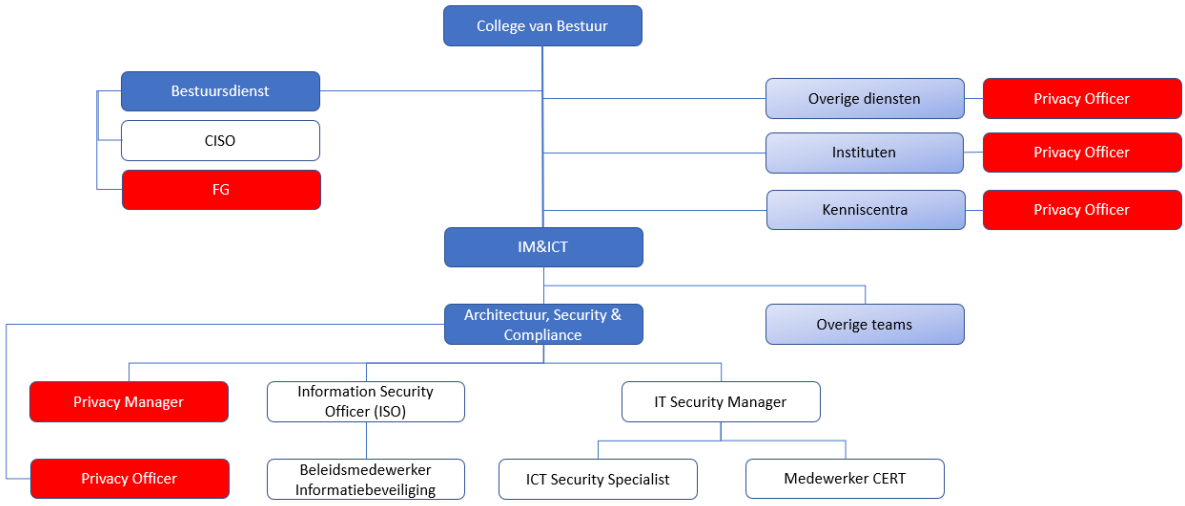
3.1 Responsibility for Privacy Policy

The EB is ultimately responsible for the privacy policy and has adopted it. The IM&ICT Service drafts the privacy policy, is responsible for implementation within the IM&ICT domain, and, where necessary, supports the directorates in carrying out and implementing the policy outside IM&ICT. The Data Protection Officer (FG) is the internal supervisor regarding compliance with the privacy policy and thus the protection of personal data. The Chief Information Security Officer (CISO) oversees and reviews HU's proper compliance with the security policy.

3.2 Roles, tasks and responsibilities

The EB is integrally responsible for the security of information (and thus personal data) within the HU's work processes. Directors are responsible for applying (or having applied) the frameworks set out in the privacy policy within their department, institute or research centre.

The overview below shows the different roles and their functional relationships.



3.2.1 The Data Protection Officer

The Data Protection Officer (Functionaris Gegevensbescherming, FG) works at the strategic level within the administrative department and is responsible, among other things, for reviewing privacy protection on the basis of national and European laws and regulations, national standards frameworks and the SURF standards framework, in line with the HU's needs and risk appetite. As part of their independent role, the FG has a direct escalation line to the Executive Board. The FG will be involved by the HU in a timely manner in all processes involving the processing of personal data. HU University of Applied Sciences Utrecht has registered the FG with the Personal Data Authority.

Assessments on the basis of the FG's board-adopted Annual Plan allow the policy and measures taken to be checked for effectiveness. Independent auditors conduct external audits. This is linked to the annual audit and is aligned as much as possible with the normal Planning & Control cycle. In addition, HU participates in SURF's benchmarks on Information Security and Privacy.

3.2.2 Privacy manager

HU University of Applied Sciences Utrecht has appointed a privacy manager to coordinate the privacy policy within the HU and ensure that the HU is broadly compliant with the GDPR and the set frameworks. The privacy manager is part of the IM&ICT Service.

The duties of the privacy manager include:

- advising on HU-wide projects and policies
- directing the privacy organisation; ensuring privacy officers have appropriate and up-to-date knowledge.
- improving and updating processes and accountability (including the processing register)
- Involve appropriate stakeholders (e.g. Procurement, IM&ICT) and connect with the privacy organisation
- In collaboration with the IT security manager and privacy officers, raise awareness among staff members and students.

Where information security and privacy intersect, the privacy manager works closely with the IT security manager.

3.2.3 Privacy officer

Each institute, department and research centre has a colleague who has taken on the role of privacy officer and has been given capacity to do so. Privacy officers are the point of contact for their own organisational unit. They advise on privacy issues and privacy dilemmas and actively inform the organisation on key GDPR topics and guidelines. Consider entering into a processing agreement or maintaining the processing register. Besides the basic tasks, most privacy officers also have a specialisation, e.g. Key user of privacy tools, consultant in conducting a DPIA or drafting a processor agreement. In addition, privacy officers take part in projects dealing with specific improvement topics (e.g. consent request process, internship and GDPR).

All privacy officers and the privacy manager collectively form the privacy organisation. They meet frequently to give further substance to the privacy policy and exchange case histories. Important

signals or issues from within the organisation are discussed if they are of interest to the HU as a whole. The privacy organisation also works on new guidelines or information that is then shared within its own organisational unit. The FG informs the privacy organisation about important issues on which it has issued advice and about issues that are HU-wide or are being taken up within SURF. It also involves the privacy organisation in its assessments where appropriate.

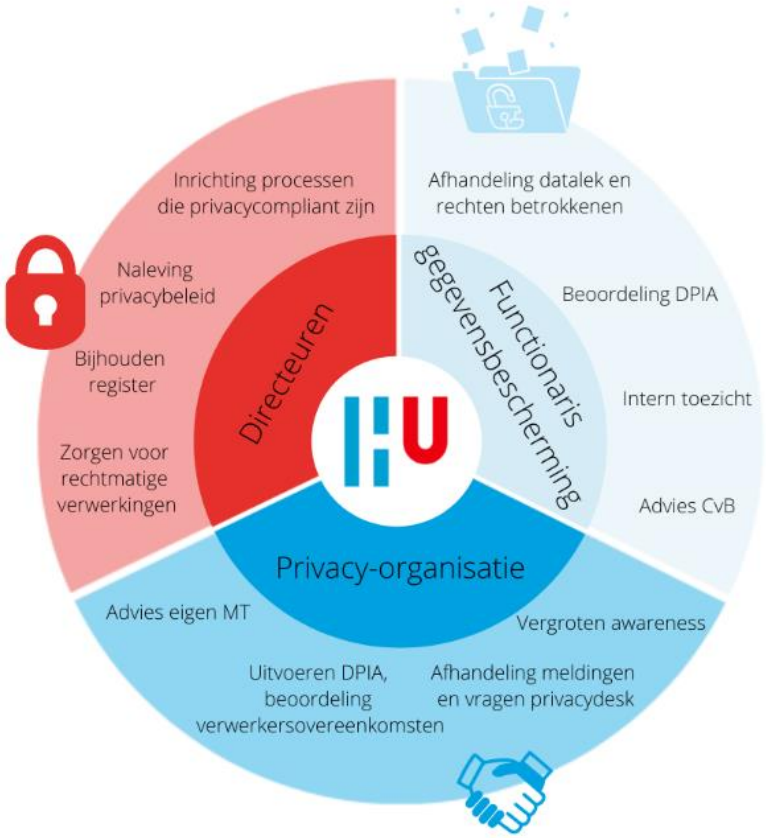
Colleagues and students can ask questions or make a report (data breach) to the privacy desk, via Askprivacy@hu.nl. These questions will be answered by the privacy officers.

3.2.4 Directors have own responsibility

Creating awareness and ensuring compliance with the policy is part of the integrated management in the institutes, services and research centres. Each director and manager - as regulated in the BBR - has the following duties:

- the role of owner of personal data ensuring lawful processing;
- maintaining an up-to-date record of processing operations;
- supporting the handling of (data breach) notifications and requests from data subjects;
- ensuring purchased tools and services comply with privacy legislation;
- authority to sign privacy agreements concerning own section.

The director is required to ensure that staff members and students are aware of key privacy guidelines by developing and managing appropriate work processes and educating/informing staff members. The in-house privacy officer can support and advise on this.



3.2.5 Collaboration within the HU

When acquiring new services and applications, privacy advice is sought and coordination takes place with Security, Sourcing, BIT consultants and Procurement. For example, on the programme of requirements and drafting processor agreements.

The Legal Affairs Department (Juridische Zaken, JZ) is regularly consulted on case histories or when developing GDPR legislation into guidelines. When starting projects and new processing operations both HU wide and within an organisational unit, the privacy officer or privacy manager advises on privacy requirements such as a DPIA or privacy statement.

CERT stands for Computer Emergency Response Team. This team has an operational task to minimise the impact of security incidents and provide support to restore the security level in a technical sense to the desired level after a security incident. When a potential data breach is (co-)caused by a security incident or when a security incident has implications for personal data, colleagues from both disciplines work closely together to investigate the data breach and take action.

In HU-wide projects involving the processing of (new) personal data, the privacy manager and the privacy officer of the relevant organisational unit are asked for advice.

3.2.6 Consultation structure

At Tactical and Operational level, structural consultations take place with the privacy officers, and JZ. IM&ICT's privacy officer participates in the Change Advisory Board (CAB) to also assess the GDPR compliance of IT changes.

An annual risk analysis for the safety domain is conducted by the information safety expert group. After weighing the defined risks, activities for the upcoming annual plan are identified. The activities are then carried out in the first line.

To ensure consistency with other safety domains, coordination takes place in periodic risk dialogues at operational, tactical and strategic levels, in line with the Strategic Framework for Integrated Safety.

The IM&ICT director participates in the tactical safety consultations. This is where directors with HU wide responsibility for a safety domain meet for policy and risk management alignment.

In the Governance consultation on information safety in which both experts from Privacy and Information Security and MT members IM&ICT participate, the progress of the Annual Plans and important HU-wide developments are discussed.

3.2.7 RACI matrix

The RACI matrix below describes the different roles from the previous section with their corresponding responsibilities.

	EB	FG	Director / Data owner	IM&ICT Director	Privacy Manager	Privacy officer	ISO
Privacy Strategy/Vision	A/I	C	C/I	R	R	C	C
Formulating privacy policy	A/I	C	I	R	R	C	C
Formulating privacy guidelines[1]	A	C	I	R	R	C	C
Drafting Annual Privacy Plan	I	C	R	A	R	C	I
Implementing policies & guidelines	A/I	C/I	R	-	C	C	C
Risk analysis and DPIA	A	C	R	-	R	C	C
Privacy assessments 1st and 2nd line (testing policy compliance)	A/I	R2	I	I	R1	C	I
Handling data breaches	A/I	C	R/I	I	C	C	C
Handling requests from data subjects	A	C	R/I	I	C	C	I
Maintaining a processing register	A	I	R	-	C	C	-
Privacy awareness	A	C/I	R	R	C	C	C

Responsible, **A**ccountable, **C**onsulted, **I**nformed

The IM&ICT Director has two roles in this model; as director and data owner (like any director) of IM&ICT and as director with information safety in portfolio (as per strategic framework Integrated Safety).

4 Approval, review and modification of privacy policy

The EB adopts the privacy policy nominated by the IM&ICT director. The HU privacy policy follows the frameworks of HU policy and is reviewed every 3 years, or after a substantial change in HU policy.

4.1 Planning Strategy & Compliance

At the beginning of the academic year, an annual plan is made by the manager Strategy & Compliance, which outlines the planning for privacy. The annual privacy plan prepared by the privacy manager is aligned with this annual plan, the recommendations from assessments by the FG and the annual Privacy risk analysis within the Information Safety domain (see also chapter 2.3.11). The Annual Privacy Plan is shared with the FG and privacy officers. The privacy officers each prepare their own annual plan, which is discussed with their own MT.

4.2 Reports

The FG reports in a half-yearly report to the Executive Board on important current developments, assessments carried out and signals, for example in response to data breaches or case histories.
The IM&ICT department reports on the realisation of the annual plan and current developments in the IR report to the EB.
A summary of these reports is shared with privacy officers and agendised in the privacy consultation with all privacy officers. Privacy manager and FG discuss key findings and progress on projects weekly.

4.3 Monitoring and compliance

The implementation of the privacy policy is reviewed annually. This is done in the autumn as part of the annual audit and is aligned as much as possible with the normal Planning & Control cycle.

The supervisory activities of the FG consist of assessing the design, existence and operation of privacy protection in existing personal data processing operations and assessing the risk assessment and lawfulness of new processing operations. Risky processing operations are reviewed with a Data Protection Impact Assessment (DPIA). The FG monitors the quality of implementation and advises on the risks and measures presented. The FG monitors the actions taken in response to a data breach. The findings are recorded in the data breach register.

The FG draws up an annual plan for assessments - testing a number of privacy processes. Think about the use of retention periods; the DPIA process or the inclusion of privacy in the curriculum. Directors are responsible for implementing the advice that follows from such an assessment. They are asked to report on this.

5 Notification and handling of privacy incidents

5.1 Definitions

A privacy incident (data breach) is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or unauthorised access to personal data transmitted, stored or otherwise processed. Any data breach must be reported to the Personal Data Authority within 72 hours of being detected. The HU has established a process for this purpose (2.3.5). The Privacy Desk and the Data Protection Officer oversee its quality and timeliness. Only those data breaches where the breach is unlikely to pose a risk to the rights and freedoms of data subjects are exempted from this notification requirement. Examples of a data breach include:

- sending a letter/email containing personal data to the wrong person;
- losing data carriers/documents containing personal data (NB even when password protected);
- stealing data carriers/documents containing personal data;
- the unauthorised accessing of personal data, e.g. staff members accessing students' personal data without authority or malicious hackers gaining access themselves; documents/files containing personal data that can be accessed through carelessness.

5.2 Incidents at the HU University of Applied Sciences Utrecht

Staff members and students can report information security incidents to the Central Service Desk (CSD). Privacy-related incidents (e.g. data breaches) can be reported to the HU's Privacy Helpdesk and to the Data Protection Officer. As soon as a privacy incident arises or has implications for information safety, both disciplines will be involved in handling the incident. If the privacy incident only affects the processing of personal data, and does not otherwise relate to information safety, the privacy organisation handles the incident further. For this, see also the data breach procedure in 2.3.5 above.

To handle a data breach properly and carefully, a data breach procedure has been established, including the investigation approach and division of responsibility, the necessary instructions and formats.

If a business process, finances or the good name of the HU are at risk, it is assessed through the line whether the EB and spokespeople should also be informed.

5.3 Supplier incidents

Information security incidents at suppliers can impact the HU. Agreements with suppliers need to specify how and when the HU is to be informed about the nature and handling of information security incidents at the relevant supplier. The processor agreement therefore contains standard agreements on the obligations of the supplier when a data breach is discovered and the contact details of the FG, to inform them as soon as possible. As the controller, the duty to report to the Personal Data Authority and, if necessary, to the data subject lies with the HU University of Applied Sciences Utrecht.

6 Sanctions

6.1 Privacy policy violations

Data and privacy code of conduct

The Data and Privacy code of conduct outlines the behaviour expected of staff members and students. This includes, for example, securely emailing confidential data, using approved apps and keeping personal data confidential. The ICT rules of conduct specifically address the use of devices, passwords, dealing with social media and reporting incidents.

Personal data security breach

The HU will not (conditionally) take legal action against reporters of (possible) security gaps in information systems. Its purpose is to get vulnerabilities in systems reported before people can/will abuse them or make the vulnerability public. Timely reporting of vulnerabilities allows the HU to take timely measures to prevent misuse. Within the HU, reporting vulnerabilities will be actively promoted.

The 'Personal data security breach notification' form also states that reporting a data breach must never affect a staff member. This is therefore the starting point. It is also possible for staff members to make an anonymous report, to make the threshold for the reporter as low as possible. Before making a report, it is not necessary for the staff member to seek prior permission or coordinate with other colleagues in advance.

A staff member cannot simply be dismissed or held liable, but HU can take action if it can be shown that the staff member acted deliberately or knowingly recklessly. For example:

- intentionally or knowingly recklessly causing a data breach,
- the deliberate concealment of a data breach when it could have been expected to have major consequences for the organisation,
- unlawful handling of personal or business confidential data; such as, for example, knowingly sharing with third parties (think of a contractor who wants to bid and may benefit from access to company data).

In these situations, labour law will have to be looked at. The Collective Labour Agreement (CAO) for Higher Vocational Education, which applies to the HU, contains several articles that apply and form part of the employment contract.

Thus, HU staff members are bound by the principle of good staff member conduct and also the duty of confidentiality.

Article P-3 of the CAO states 'the staff member may impose a disciplinary measure on a staff member who fails to do or refrain from doing what a good staff member required to do or refrain from doing in similar circumstances and/or is guilty of dereliction of duty'. In a situation where the principle of good employee conduct or the duty of confidentiality is not met, the appropriate measures can be assessed in consultation with HR and JZ.

In addition, it is important to mention that if a staff member fails to report a data breach, there may also be consequences for the staff member but also for the HU. For example, the Personal Data Authority can fine the HU for failing to report a data breach.

Information security breach

Measures may be taken by or on behalf of the EB in case of violation of the rules regarding information security. Measures could include blocking access to the network or specific network services. In case the HU is sued for violation of intellectual property rights or other regulations, or for violation of rights of others, the HU may recover any damages from the user who caused the damage. If damage is suffered as a result of misuse of computer and network facilities, the HU may also recover them from the user who caused the damage.

Appendix 1: Glossary

***GDPR**:* General Data Protection Regulation

Personal Data Authority (Autoriteit Persoonsgegevens, AP): the Dutch supervisory authority on the processing of personal data.

***Concerned**:* an individual and natural person to whom a personal data relates.

Data breach: a breach of the security of personal data leading to any unauthorised processing thereof. A data breach can be caused either intentionally or unintentionally.

Data Privacy Impact Assessment (DPIA): An assessment that helps identify privacy risks and provides the tools to reduce these risks to an acceptable level.

Third party: any other person, other than the data subject, the controller or the processor, or

any person under the direct authority of the controller or processor

and authorised to process personal data.

Joint controller agreement: a processor agreement where there are two controllers who have joint purposes in a processing operation. For example, consider a research project where multiple parties are processing data for the same (research) purpose.

Minor: any person who has not yet reached the age of 18 years.

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

Privacy by Default: a data processing operation in which the default settings of products and services are set in such a way that the privacy of data subjects is maximised. This includes requesting and processing as little data as possible.

Privacy by Design: The management of a processing operation of personal data, from collection to processing and deletion, with mechanisms designed to take the privacy of data subjects into account as much as possible. Here, systematic attention is paid to comprehensive safeguards regarding accuracy, confidentiality, integrity, physical safety and deletion of personal data.

Privacy Statement: A notice explaining in understandable language to data subjects what personal data is processed and in what way.

Privacy Shield: The Privacy Shield provided a guarantee that a supplier (in the US) complied with the requirements from the GDPR. This Privacy Shield has since been declared invalid by the European Court, because the privacy guarantees, among other reasons, could not be realised due to national legislation in the US.

Profiling: any form of automated processing in which, on the basis of personal data, certain personal aspects of a natural person are evaluated, in particular with a view to analysing or predicting his professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

Standard Contractual Clause (SCC): Processor agreement for companies (in the US) outside the EEA, for which their legal arrangements do not provide the same safeguard as the GDPR. An SSC is modular and can also apply in the case of a joint controller agreement.

Processor: a party engaged by the HU University of Applied Sciences Utrecht who processes personal data on behalf of the HU University of Applied Sciences Utrecht, and on the basis of its written instructions.

Processing: any act or set of acts relating to personal data, including the collection, recording, organisation, storage, consultation, updating, blocking, erasure or destruction of data.

Controller HU: The Executive Board of HU University of Applied Sciences Utrecht which determines the purpose and means of processing personal data.

Appendix 2: Laws and regulations

At the HU, relevant laws and regulations are dealt with in the following manner.

General Data Protection Regulation (GDPR)
Since 2012, new legislation on privacy, the GDPR, has been in the works at European level. In May 2016, this regulation was officially published, and a 2-year implementation period started. This means that from 26 May 2018, anyone processing personal data within Europe must comply with this regulation. Compliance with security measures and expected behaviour leads to compliance with the law.

The General Data Protection Regulation calls for extra attention to the processing of special personal data, including health data. A healthcare institution is therefore obliged to adequately protect its clients' data on file. In fact, this has made the said NEN standards implicitly mandatory for the healthcare sector for many years (since 2005) in the context of personal data security. The healthcare information security standard therefore applies to all healthcare providers and organisations in the healthcare and welfare sector that manage personal health information (such as the HU), regardless of the nature and scope of the business process.

General Data Protection Regulation Implementation Act (GDPR Implementation Act)
The GDPR is a European regulation. This means that the GDPR does not need to be incorporated separately into Dutch legislation once again. The GDPR does impose an obligation on EU member states to regulate certain matters (such as the establishment of a national authority to supervise), and also allows them to flesh out certain standards and rules in the GDPR. The General Data Protection Regulation Implementation Act fills in these standards and rules for the Dutch situation. The GDPR Implementation Act is, among other things, the legal basis for the establishment, tasks and responsibilities of the Personal Data Authority, but also contains detailed provisions for the processing of special personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning health, or data relating to a person's sexual behaviour or sexual orientation)

Higher Education and Research Act [Wet op het Hoger onderwijs en Wetenschappelijk onderzoek, WHW]
The HU has a quality assurance system (ITK), in which (among other things) the careful handling of data in student administration and study results is guaranteed. In addition, codes of integrity for scientific research are observed and applied.

Medical Treatment Contracts Act [Wet op de geneeskundige behandelovereenkomst, WGBO]
The WGBO (Dutch Civil Code book 7, division 5, section 446-468), regarding rights and obligations for both caregiver and client, applies to the processing of data by the healthcare institution obtained by the caregiver in the context of treatment of the client. That law requires him to record the necessary data in his file on the client.

Public Records Act [Archiefwet]
The HU complies with the regulations of the Public Records Act and the Public Records Decree on how to handle information recorded in (digitised) documents, information systems, websites, etc. This is periodically part of the external auditors' reports.

Copyright Act [Auteurswet].
The HU does not distribute original works without obtaining permission from the copyright owner. This also implies that the HU prevents the use of software without owning the appropriate licences.

Computer Crime Act III [Wet Computercriminaliteit III]
The Computer Crime Act III focuses on the criminal law problem areas related to computer use. The law requires 'some security' before there can be any criminal prosecution of offences against the educational institution and any indemnification of directors of the institution.

Compliance with this information security policy and implementation of the measures as named in the IB Higher Education Standards Framework) at HU leads to a level of security that may be considered sufficient under the Computer Crime Act III.

If attacks on the HU take place that significantly breach security and are covered by the Computer Crime Act III, the HU will in principle file a report, unless the attack was explicitly intended to demonstrate weaknesses in the security of the HU systems, the weaknesses identified were not actively abused and the HU was informed of the activities and results in a timely manner. The MT IM&ICT and HU-CERT coordinator advise the EB in this regard. The EB may take the decision to file a report.

If the HU's information resources are misused by staff members, students, partners or other third parties to commit criminal offences, the HU will in principle file a report. . The MT IM&ICT and HU-CERT coordinator advise the EB in this regard. The EB may take the decision to file a report.

Other guidelines and national agreements
As stated earlier, the information security policy at the HU is based on the SURF Standards Framework. HU complies with the following guidelines and national agreements:

- Dutch code of scientific integrity (Nederlandse gedragscode wetenschappelijk integriteit, NGWI), 2018
- Higher Education Standards Framework, 2017
- SURFnet user agreement, 2018
- Risk analysis higher education institutions, 2017

Appendix 3: List with abbreviations:

GDPR: General Data Protection Regulation

GDPR Implementation Act: General Data Protection Regulation Implementation Act

DPIA: Data Protection Impact Assessment

EER: European Economic Area

SCC: Standard Contractual Clause

SCIPR: SURF Community for Information Security and Privacy

IVHO: Integrated Safety Consultation Higher Education

FG: Data Protection Officer

WHW: Higher Education and Research Act

ISO: International Organization of standardization

EC: European Commission

CERT: Computer Emergency Response Team

CISO: Chief Information Security Officer

JZ: Legal Affairs

PDCA: Plan-Do-Check-Act

BIT consultant: Business Information Technology consultant

AP: Personal Data Authority

CSD: Central Service Desk

ISO: Information Security Officer