GENERAL POLICY ON THE PROTECTION OF PERSONAL DATA

UNIVERSITY OF GRONINGEN

Contents

1. Starting points

1.1. Introduction

Due to advancing digitization and increasing awareness of the importance of protecting an individual's private life, privacy has become more relevant than ever. One corollary of the right to privacy is the obligation to handle personal data properly and carefully. The Board of the University wants this obligation to be honoured throughout the University of Groningen. To that end, the Board of the University has adopted a general policy on protection of personal data (hereinafter: privacy policy), which outlines the vision and principles of the University of Groningen regarding the protection of personal data.

A list of definitions of the terms used can be found in Section 4 of this policy document.

1.2. University of Groningen's views on privacy

The UG's mission is to create and share knowledge through excellent research and teaching. The UG thus wants to make a substantial contribution to society. The UG's views on privacy are in line with this mission.

All students, staff, research subjects and other individuals associated with the UG must be able to trust that their personal data will be lawfully processed and adequately protected by the UG. Personal data that are processed within the UG will be handled carefully and properly at all times. Compliance with the applicable privacy laws and regulations enables the UG to provide a consistent, high level of protection of the rights and freedoms of individuals ('privacy maturity').

The UG is therefore transparent about what it does with personal data and will assume responsibility, including when mistakes are made. The UG allows individuals to inspect and correct their data. Their questions and possible complaints will be taken seriously and will be properly dealt with.

Within this framework, excellence in teaching and research is fostered and realized as much as possible. Privacy maturity contributes positively to the UG's mission.

1.3. Purpose

The purpose of this privacy policy is:

- To ensure that the personal data that the UG processes are handled in a careful, proper and safe way that is in accordance with the applicable privacy laws and regulations and respects the rights and freedoms of individuals
- To create the frameworks within which this policy will be implemented
- To prevent privacy incidents and, if they do occur, limit the damage for individuals and the organization
- To implement measures and mechanisms that optimize the UG's privacy maturity

- To facilitate and activate all staff members of the UG to contribute to the privacy maturity of the organization
- To enable the Board of the University to be confidently accountable to those concerned and to the authorities.

1.4. Target group

The target group for this policy includes all UG staff members and students. The responsibilities, tasks, and competences of staff members and students with regard to the protection of personal data are further elaborated in this privacy policy and the related guidelines, regulations, and codes of conduct. For the sake of transparency about the processing of personal data, the policy is published on the public website of the UG.

1.5. Scope of application

This privacy policy applies to the processing of personal data. Personal data are all data relating to a natural person that identify this person directly or indirectly. Processing concerns all actions relating to personal data, such as viewing, sharing, modifying, copying, storing, and destroying data. The policy covers the entire life cycle of personal data. The policy applies to both automated and non-automated processing.

The policy applies to the University as a whole and to all its faculties, service units, and departments. It is aimed at all processes within the University where personal data are being processed, both in the context of teaching and research and in the context of facilitating and supporting these primary tasks. This policy also applies when the processing of personal data is carried out by a third party on behalf of the UG, jointly with the UG, or otherwise by or on behalf of the University.

1.6. Overlaps with and relationship to other policy themes and policy documents

This privacy policy overlaps with other policy areas within the UG. It has been aligned as much as possible with the policy drawn up for these other areas. It is possible, however, that in these documents other emphases are placed on the protection of personal data. These must always be assessed in the light of this privacy policy.

1.7. Legal framework

The legal framework for this privacy policy is primarily based on the General Data Protection Regulation (hereinafter: GDPR). In addition, there is national implementing legislation (e.g. the Dutch GDPR Implementation Act) and legislation that lays down rules for specific ways to process personal data. Furthermore, there is legislation that provides specific instructions with regard to processing, such as storage obligations (e.g. Article 52 of the Dutch State Taxes Act (*Algemene wet inzake rijksbelastingen*, AWR) or anonymization requirements (e.g. Article 10.1.d of the Dutch Government Information Act (*Wet openbaarheid van bestuur*, Wob). Needless to say, other legislation that the UG must comply with (e.g. the Dutch Higher Education and Research Act or the General Administrative Law Act) may also form part of the legal framework. However, it would go beyond the bounds of this policy document to determine the interrelationships between the various legislative acts. These will be assessed on a case-by-case basis.

In addition to the applicable legislation, the legal framework is determined by policy rules, codes of conduct, and certification mechanisms established by a competent government agency (e.g. the Dutch Data Protection Agency). This also applies to the views of the Data Protection Officer (hereinafter: DPO). Codes of conduct may also be drawn up by umbrella organizations such as the VSNU (e.g. Code of conduct for the use of personal data in academic research) or by the UG itself, to which the University will commit itself.

1.8. Date of coming into effect and maintenance

The first version of this privacy policy was established on 4 June 2018 by the Board of the University and took effect on that date. The policy will be supplemented and amended from time to time. Amendments will take effect after approval by the Board of the University. The changes in this version mainly concern the structure of the privacy management organization. The work plan cycle has been amended slightly and the roles of Chief Privacy Officer and IT auditor have been embedded in the privacy management organization.

2. Privacy management

2.1. Management structure

The UG can only become privacy mature if all levels of governance and all staff members of the University comply. That is why this policy is deliberately activating in nature and why the UG has a structure that makes privacy management possible. This structure has been determined on the basis of a RASCI Responsibility Matrix:

	Type of responsibility	**Position**
Responsible	Factual responsibility	Faculty board / service unit management
Accountable (approving)	Ultimate responsibility	Board of the University
Supporting	Executive responsibility	Privacy & Security coordinators, researchers, staff and students of the UG
Consulting	Advisory responsibility	CPO, ABJZ, CISO
		DPO, IT auditor
		Strategic Committee for Privacy Protection and Information Security
Informed	Informed responsibility	Consultative participation bodies, data subjects, external supervisors[1]

A further elaboration of these responsibilities in scope, duties, and competences will be given in the remainder of this policy document. The respective faculty board or service unit management will always provide the person(s) charged with one or more of the duties described above with the required means and time to properly perform these duties.

2.2. Responsibilities and competences of the faculty boards and service unit managements

The UG faculty boards and service unit managements are responsible for ensuring that their faculty or service unit complies with the applicable privacy legislation and this privacy policy. They are charged with the following duties and responsibilities:

- Raising awareness of the importance of privacy maturity for their respective faculty or service
- Taking stock of all processing of personal data within their faculty or service, registering these processing operations in the appropriate register, and keeping these records up-to-date

[1] Section 3.11 of this policy describes how the UG renders account to data subjects and supervisors.

- Mapping, assessing, and mitigating the risks for the protection of personal data that are involved in the processing of such data by the organizational unit
- Ensuring that the processing of personal data is in accordance with privacy laws and regulations
- Ensuring that a DPIA (Data Protection Impact Assessment) is performed and/or that the DPO is consulted in good time if this is necessary under the privacy laws and regulations or UG policy
- Based on a risk analysis, realizing appropriate safeguards for the protection of personal data
- Monitoring the privacy maturity of their faculty or service
- Reporting actual and suspected data breaches and privacy incidents within the faculty or service unit in full and in good time
- Coordinating the application of this policy with other faculties and service units in order to prevent duplication of work.

Each faculty board or service unit management will establish an annual plan of approach, detailing the above-mentioned responsibilities in terms of concrete measures and activities for the domains of teaching, business operations, and academic research. This plan of approach forms part of the work plan for personal data protection and information security, which each faculty and service unit must draw up every year on the basis of the University guidelines for drawing up work plans for information security and data protection.

The faculty boards are specifically responsible for protecting the personal data that are processed in the context of academic research. The faculty boards support researchers in carrying out their responsibilities.

Privacy is an independent focus area of a faculty board or service unit management. If a faculty board or service unit management consists of more than one person, a decision will be made as to who will be the privacy officer.

Each faculty board or service unit management will appoint at least one Privacy & Security coordinator to coordinate the implementation of the privacy laws and regulations and this privacy policy within its faculty or service unit. Where necessary, the board or management will appoint several privacy & security coordinators, for example for certain departments. A faculty board or service unit management may choose to create a privacy committee for its faculty or service unit. This committee will be made up of the privacy officer on the board or management and the privacy & security coordinators.

The faculty boards and service unit managements are accountable to the Board of the University. They must ensure that their annual work plans discuss the realization of intended activities and measures in the year prior to the year covered by the work plan. ABJZ will receive a copy of this report, which will be assessed on behalf of the Board of the University by the Chief Privacy Officer (hereinafter: CPO), the Chief Information Security Officer (hereinafter: CISO), the DPO, and the IT auditor.

2.3. Responsibilities and competences of the Board of the University

The Board of the University has ultimate responsibility for the management of the University databases and the privacy maturity of the University of Groningen. In this context, the Board of the University is the point of contact for the external supervisor, the data subject concerned, and third parties, and thus assumes responsibility to the public at large. Where necessary, the Board of the University will also inform the University Council and the Supervisory Board of developments in this area. The Board of the University may be assisted by the DPO when rendering account and providing information. The Board of the University establishes policy to determine how the DPO can be sufficiently involved in good time in matters concerning the protection of personal data.

The Board of the University annually evaluates the UG's growth in privacy maturity on the basis of the DPO's annual report. This evaluation is communicated in the form of a management response to the report, which is prepared by the CPO. The Board of the University facilitates the committees and staff members of the UG in complying with the privacy laws and regulations and will make resources and support available for this. If a faculty board or service unit management breaches privacy laws and regulations or this privacy policy, the Board of the University will implement reasonable measures or sanctions to rectify this.

2.4. Responsibilities and competences of privacy & security coordinators, process managers and staff members

2.4.1. General provisions

Privacy & security coordinators, process managers, researchers, and staff members operate under the responsibility of their faculty board or service unit management.

2.4.2. Responsibilities and competences of privacy & security coordinators

Every faculty or service within the UG has at least one privacy & security coordinator who supports the process of making their faculty or service unit privacy mature and coordinates the execution of the duties of their board or management. The Privacy & Security coordinator is the first point of contact for privacy-related questions from staff members of the faculty or service unit. The coordinator also records and registers the processing of personal data in the appropriate register. The Privacy & Security coordinator is accountable to their board or management.

2.4.3. Responsibilities and competences of staff members

All staff members of the University of Groningen must handle the personal data they process with care. They must take note of the relevant policy documents, guidelines, and instructions drawn up for this purpose and comply with them. Where necessary and possible, they support the organization with their knowledge and expertise. When they become aware of any privacy incidents, they must report these as quickly as possible to the designated reporting point or the DPO.

2.4.4. Responsibilities and competences of researchers

Each researcher has an independent responsibility for the privacy maturity of their research. In fulfilling this responsibility, the ethics committees have a role to play. They are responsible for assessing the research in terms of ethical and legal requirements on behalf of the faculty board. Each researcher must comply with the privacy laws and regulations, professional codes of conduct, and faculty policy. In addition to the regular support within the faculty, support is provided by the Groningen Data Competence Center (hereinafter: GDCC).

2.4.5. Responsibilities and competences of students

Students of the UG may be given access to personal data in the context of their degree programme. Students must handle these personal data with care and comply with the University policy and the instructions that they receive from their lecturers and supervisors. Faculties are responsible for supervising students in the use of personal data in research.

2.5. Responsibilities and competences of the CPO, ABJZ, and the CISO

2.5.1. Responsibilities and competences of the CPO

The Chief Privacy Officer (CPO) is responsible for developing and implementing the University privacy policy, including guidelines and procedures for the protection of personal data of students, staff, research subjects, and other individuals. The CPO ensures that the faculties and service units act in accordance with this policy and that the measures resulting from it are applied. The CPO issues advice to faculties and service units in drawing up and implementing the work plan and provides content-related support to the privacy & security coordinators. The CPO issues advice to the Board of the University about the implementation of annual reports and the DPO's recommendations.

The CPO issues advice about complex privacy matters, initiates risk analyses and privacy audits, organizes awareness programs, and issues advice to the administration and management. The CPO ensures an overview and management of the privacy risks that are relevant within the UG. The CPO reports on their activities to the Strategic Committee for Privacy Protection and Information Security, and is employed by the department of ABJZ.

2.5.2. Responsibilities and competences of ABJZ

ABJZ issues advice to faculties and service units about the implementation of privacy laws and regulations within the UG. ABJZ supports DPIAs, draws up processor agreements, and develops privacy statements. ABJZ supports all staff members and in particular the privacy & security coordinators, process managers, researchers, and the DPO in performing their duties. ABJZ issues advice to researchers entering collaborations about compliance, exemptions that apply to research, and preconditions defined by research funders. ABJZ issues advice on the further elaboration of this privacy policy. ABJZ continuously coordinates their work with the DPO, CPO, and CISO.

2.5.3. Responsibilities and competences of the CISO

The Chief Information Security Officer (CISO) is responsible for developing and implementing the University information security policy, including guidelines and procedures for protecting the University information systems against internal and external threats. The CISO is responsible for the functioning of the Information Security Management System and monitors the University's compliance with the information security policy. The CISO reports on this to the Strategic Committee for Privacy Protection and Information Security. The CISO is employed by the CIT.

The CISO supports the UG in taking appropriate technological and organizational measures to protect personal data against unauthorized access and unlawful processing. The CISO is chair of the UG Computer Emergency Response Team (CERT).

2.6. Responsibilities and competences of the DPO and the IT auditor

2.6.1. Responsibilities and competences of the DPO

The DPO is responsible for issuing solicited and unsolicited advice about compliance with the privacy laws and regulations and the privacy policy, as well as for supervising this compliance. Within the UG, the DPO has, as a minimum, the duties, responsibilities, and competences that are assigned to them under the privacy laws and regulations.

The DPO has access to all information from the UG relating to the processing of personal data – both to the personal data themselves and to the processing operations and systems with which these activities are performed. The Board of the University may determine that in order to obtain access to certain information, prior notification of the Board of the University is required. The DPO supervises the register for the processing activities.

The DPO is empowered to perform tasks and to keep their expertise up to date. The DPO reports directly to the Board of the University. The DPO annually reports on the protection of personal data within the UG. This report is made available to the Board of the University and the Supervisory Board, and sent to the University Council for information purposes.

The DPO supports the Board of the University in rendering account externally, both to supervisors and to those concerned. To that end, the DPO maintains contact with the supervisory authorities. The DPO provides recommendations aimed at further optimization of the privacy policy.

2.6.2. Responsibilities and competences of the IT auditor

The internal IT auditor monitors risk management and the effectiveness of risk-mitigating measures with regard to University processes and information systems. At the request of the Board of the University and the DPO, the UG IT auditor assesses the structure, existence, and operation of the UG privacy policy and the measures for mitigating the risks for the protection of personal data. The IT auditor enters these activities into a University audit plan. The IT auditor reports on their activities to the Strategic Committee for Privacy Protection and Information Security.

2.7. Responsibilities and competences of the Strategic Committee for Privacy Protection and Information Security

The Strategic Committee for Privacy Protection and Information Security issues advice to the Board of the University about the development of University-wide policy and work programmes in the field of privacy and information security. The Committee ensures that data protection and information security are in accordance with the UG's strategic aims. The Committee issues advice to the Board of the University about the UG's risk strategy and the requirements for satisfying legislation and regulations. The Committee consists of one member of the Board of the University (also the chair), two members of the Management Council, the CISO, and the CPO. The IT auditor and the DPO function as advisory members.

2.8. Responsibilities and competences of the consultative participation bodies

Insofar as required by law or internal policy, the consultative participation bodies of the UG are empowered to exercise their competences with regard to how the UG implements privacy laws and regulations.

3. Implementation of privacy policy

3.1. Board of the University privacy maturity work programme and policy evaluation

The UG uses a standard model for privacy maturity: the 'Privacy Maturity Model' drawn up by the Center for Information Security and Privacy Protection. The UG has set itself the goal of acting at a maturity level of at least 3.0 on average in accordance with this model, thus achieving the mission, vision, and aims formulated in Chapter 1. The model is applied bearing in mind the structure and culture of the organization. The Board of the University defines annual work plans discussing what needs to be done in order to achieve and maintain the desired level in response to the DPO's annual report and the privacy maturity level of the University. The CPO prepares the work programme, embeds its implementation in the University *Plan-Do-Check-Act* cycle for data protection, and ensures that it is also embedded in the work plans of the individual faculties and service units.

3.2. PDCA cycle, work plans of faculties and service units

The faculty boards and service unit managements are responsible for implementing a *Plan-Do-Check-Act* cycle that enables them to achieve and maintain privacy maturity for the processes within their faculty or service unit. In this context, they determine how and when they implement the tasks and responsibilities described in Section 2.2. To this end, they draw up annual work plans in accordance with the University guidelines for drawing up work plans for information security and data protection and the instructions given by the CISO and CPO. With these work plans they carry out the duties and responsibilities of the faculty boards and service unit managements in terms of concrete activities and measures with regard to processes and systems with the aim of further optimizing the faculty or service unit's privacy maturity. The work plans are sent to the Board of the University and assessed on its behalf by the UG's DPO, CPO, IT auditor, and CISO. The faculty board or service unit management will receive feedback on this assessment. The assessment is sent to the Board of the University and discussed in the Management Council, and subsequently sent to the Committee of Deans for information purposes. ABJZ coordinates this process.

3.3. Privacy by design & by default, DPIAs

Innovative research projects and new processes within the UG, as well as the systems that support these processes, are designed in such a way that the privacy impact is as low as possible while continuing to achieve the legitimate objectives of these processes. Privacy by design and privacy by default are part of the process of purchasing, developing, and implementing information systems.

Where necessary, a DPIA will be carried out. The UG has a protocol that determines when this is mandatory and that encourages the sharing of insights from the DPIAs. As a minimum, the protocol must be in line with the requirements of the privacy laws and regulations and stipulate when the support of ABJZ is required. Faculty boards and service unit managements are responsible for compliance with this protocol. When a DPIA has been carried out, this will be recorded in the register referred to in Section 3.5.

3.4. Codes of conduct and certifications

Where possible and reasonable, the UG will conform with codes of conduct and certification requirements that promote the careful and proper handling of personal data. The Board of the University decides in its annual work programme to which codes of conduct the UG will adhere. The DPO may advise the UG to conform with codes of conduct.

3.5. Register for the processing activities

All processing of personal data by or on behalf of the UG is recorded in a central register under the responsibility of ABJZ. This register complies with the requirements of privacy laws and regulations, but is also an instrument to achieve privacy maturity and to be accountable for this. ABJZ, in consultation with the CPO and DPO, ensures that the register can be used for this purpose and determines the information to be recorded. The register is suitable for all processing operations carried out by the UG, both in its capacity as responsible party and as processor within the meaning of the privacy laws and regulations.

3.6. Information security

The information security policy of the UG and the underlying set of measures provide adequate protection of personal data against unlawful processing and unauthorized access. The measures are both technical and organizational in nature. The information security policy applies to all processing of personal data by the UG, with or without the use of external parties (processors) or jointly with another responsible party. In the context of the information security policy, personal data will at least be classified as ‘confidential’. However, for each process in which personal data are processed, it will be assessed whether this security level is appropriate. Faculty boards and service unit managements are responsible for this.

3.7. Privacy incidents

Actual or presumed data breaches and security or other incidents that violate the protection of personal data must be reported to a designated reporting point at the CIT. The notifications are handled in accordance with the Protocol for Mandatory Notification of Data Breaches of the UG. This protocol is annually evaluated by the CPO, the CISO, and the DPO. Reported data breaches are recorded in the register referred to in Section 3.5.

3.8. Processing of the UG’s personal data by third parties

The UG may outsource the processing of personal data to third parties, perform the processing jointly with third parties, or provide the personal data to third parties. ABJZ provides support in assessing the legality of data provision. If it is decided to let a third party process personal data, written agreements will be made with this party to ensure careful and proper handling of the personal data. The agreements must comply with the requirements of the privacy laws and regulations, including Articles 26 and 28 of the GDPR. In consultation with the DPO, ABJZ will develop model agreements that can be used by UG staff members to submit to third parties. The actual conclusion of agreements must always take place in accordance with ABJZ's instructions. The agreements are signed by or on behalf of the Board of the University. ABJZ and the DPO will play a coordinating role in multi-institutional collaborations on agreements concerning the processing of personal data. ABJZ will draw up a process to monitor compliance with processor agreements.

3.9. International exchange of data

The processing of personal data outside the European Economic Area (EEA) is only possible if appropriate safeguards are in place for the protection of personal data according to the privacy laws and regulations. Prior to such processing, the DPO or ABJZ will always give instructions for arranging these safeguards.

3.10. Transparency and accountability

3.10.1. Privacy statement

The UG will inform data subjects in full, in time, and in understandable language about the processing of their personal data. There is a UG-wide privacy statement which will be brought to the attention of the data subject prior to the processing of their personal data.

For specific data processing, the data subject concerned must also be presented with a specific privacy statement that complements and refers to the UG-wide privacy statement. The faculty boards and service unit managements are responsible for ensuring that this specific privacy statement is drafted and submitted. They coordinate this with the DPO or ABJZ. In the case of academic research, this is done in coordination with the ethics committee. Such a complementary privacy statement will in any case be drawn up when the data are processed on the basis of the data subject's permission. Complementary privacy statements are registered with ABJZ.

3.10.2. Rights of data subjects

All requests, questions, and complaints from a data subject regarding the UG's processing of personal data must be assessed and settled in a timely, careful, and proper fashion. A Central Privacy Desk has been set up for this purpose at ABJZ. There is a protocol for the handling of messages and notifications submitted to the Privacy Desk. This protocol describes how the data subject's requests will be handled under the privacy laws and regulations (for example, a request for access or a request for deletion of personal data). In each privacy statement, data subjects will be informed about their rights and about the Central Privacy Desk.

3.10.3. Accountability to privacy supervisors

The Board of the University is accountable to the competent national and international privacy supervisors and the Supervisory Board. The Board of the University is responsible for providing all relevant information and making the UG's privacy maturity transparent.

3.11. Communication and PR

All staff members will be informed of this privacy policy and the associated duties and responsibilities they bear. To this end, a portal has been set up on the UG's intranet. The website will contain information about privacy laws and regulations, work instructions, and model contracts. In addition, the public UG website contains information on the handling of personal data and on its views on privacy. The information is prepared and updated by the Communication Department of the Office of the University, in collaboration with ABJZ.

In the event of a privacy incident or other privacy-related PR issue, the Board of the University will be accountable to all data subjects, the supervisor, and other stakeholders. The DPO may render account on behalf of the Board of the University, always in consultation with the Board of the University.

3.12. Raising awareness and training

The UG works continuously to raise staff awareness of privacy maturity. For example, guidelines have been drawn up that encourage the careful handling of personal data. All UG staff members are given the opportunity to follow a training course in which they are informed of the relevant sections of the privacy laws and regulations.

3.13. Nature of this privacy policy

This privacy policy provides general guidelines for achieving privacy maturity, but does not describe the conditions that may apply to specific processing activities. For each processing activity, it is necessary to consciously and separately examine how it is aligned with legislation and regulations as well as this policy.

3.14. Implementation and further elaboration of privacy policy, guidelines

Any competence to deviate from this privacy policy will be explicitly mentioned in this policy.

ABJZ will draw up University-wide guidelines on behalf of the Board of the University and in collaboration with the privacy & security coordinators to prescribe how staff members, process managers, or privacy & security coordinators must act when handling personal data. Faculty boards or service unit managements may do this for their individual faculty or service. If necessary, ABJZ will consult the CPO, DPO, and/or CISO before approving a guideline.

4. Definitions of terms used

The terms used in this Privacy Policy are defined as follows:

- ABJZ: *Algemeen Bestuurlijke en Juridische Zaken*; the Department of General Administrative and Legal Affairs of the UG
- GDPR: the General Data Protection Regulation
- Data subject: a natural person whose personal data are being processed

- CISO: the Chief Information Security Officer of the UG
- CPO: the Chief Privacy Officer of the UG
- Board of the University: the Board of the University of Groningen
- DPIA: Data Protection Impact Assessment: an assessment of the privacy impact of a process or system in which personal data are processed
- DPO: the Data Protection Officer of the University of Groningen
- Groningen Data Competence Center (GDCC): a collaboration between the University Library and the Center for Information Technology of the University of Groningen to support researchers and research institutes in managing their data
- Personal data: all data relating to a natural person and identifying this person directly or indirectly
- Privacy maturity: complying with the privacy laws and regulations and safeguarding a careful and proper handling of personal data
- Privacy & Security coordinator: a UG staff member designated by a faculty board or service unit management to coordinate the privacy maturity of a faculty, service unit, or department thereof
- Privacy statement: a statement, form for informed consent, or any other document informing a data subject about the processing of their personal data by the UG
- Privacy laws and regulations: all national or international laws and regulations that apply to the UG and stipulate conditions regarding the processing of personal data, including the GDPR
- Process manager: a UG staff member who bears responsibility for the implementation of a process or several related processes within a faculty or service unit, or for the systems supporting these processes
- Privacy policy: this general policy on the protection of personal data at the UG
- Privacy impact: the adverse consequences of a process or processing operation for the careful and proper handling of personal data and for the protection of the privacy of a data subject
- UG: the University of Groningen
- Strategic Committee for Privacy Protection and Information Security: the strategic committee that issues advice to the Board of the University about the application of this privacy policy in relation to the UG's strategic aims
- Processing, processing operation: every act/action with regard to personal data, such as viewing, sharing, changing, copying, storing, and destroying data
- Processor: every person, legal entity, or organization who/that processes personal data on behalf of the UG.

Last changed on 29 November 2021.