version 1.0 4 June 2018

GENERAL POLICY ON PROTECTION OF PERSONAL DATA

UNIVERSITY OF GRONINGEN

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.

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 and in a way that, at the very least, complies with the privacy laws and regulations ('privacy-proofness').

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-proofness 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 applicable privacy laws and regulations
- To create the frameworks within which this policy will be implemented
- To prevent privacy incidents and, if they occur, limit the damage for those concerned and the organization
- To implement measures and mechanisms that optimize the UG's privacy-proofness
- To facilitate and activate all staff members of the UG to contribute to the privacy-proofness 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 is all UG staff members. The responsibilities, tasks and competences of staff members 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). Of course, if applicable, other legislation that the UG must comply with (e.g. the Dutch Higher Education and Research Act or the General Administrative Law Act) also forms 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 scientific research) or by the UG itself, to which the University will commit itself.

1.8. Date of coming into effect and maintenance

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.

2. Privacy management

2.1. Management structure

The UG can only become privacy proof 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 Directorate
Accountable (approving)	Ultimate responsibility	Board of the University
Supporting	Executive responsibility	Privacy & security - coordinators / Process managers / researchers / UG staff members
Consulting	Advisory responsibility	DPO
		IT lawyer / Security Manager
Informed	Informed responsibility	Consultative participation bodies, parties concerned, 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 Board of 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 Board / Service Unit Boards

The faculty boards and service directorates of the University of Groningen are responsible for ensuring that their faculty or service unit is privacy proof and complies with this privacy policy. The board or the directorate is charged with the following duties and responsibilities:

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

- Raising awareness of the importance of privacy-proofness for their respective faculty or service unit
- Taking stock of all processing of personal data within their faculty or service unit, registering these processing operations in the appropriate register and keeping these records up-to-date
- 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 when necessary under the privacy laws and regulations or UG policy
- Realizing appropriate safeguards for the protection of personal data, including taking security measures, informing data subjects and recording written contractual agreements with processors
- Monitoring the privacy-proofness of their faculty or service unit
- The timely and complete reporting of data breaches and privacy incidents, actual or suspected, within the faculty or service unit.

The board of a faculty is specifically responsible for the privacy-proofness of processing personal data in the context of academic research. The faculty board supports the researcher in carrying out his/her responsibilities.

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

The faculty board or service directorate 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 faculty board or service directorate will appoint several privacy & security coordinators, for example for certain departments. A faculty board or service directorate may choose to create a privacy committee for its faculty or service unit. This committee will be made up of the person in charge of the privacy portfolio on the board or directorate and the privacy & security coordinators.

The faculty boards and service directorates are accountable to the Board of the University. They report at least annually to the Board of the University about the performance of their duties and responsibilities pursuant to this privacy policy and about the executed and planned DPIAs. The DPO will receive a copy of this report.

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-proofness 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 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 will lay down in an annual work programme how it intends to optimize privacy-proofness. 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 directorate acts in violation of the 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. Responsibilities and competences of privacy & security coordinators

Every faculty or service unit within the University of Groningen has at least one privacy & security coordinator who supports the privacy-proofing of that faculty or service unit and coordinates the execution of the duties of their board or directorate. The privacy & security coordinator is the first point of contact for privacy-related questions from staff members of that faculty or service unit. The privacy & security coordinator is accountable to their board or directorate.

Where necessary, the privacy & security coordinator calls in the help of the DPO, the IT lawyer or the Security Manager when performing his/her duties.

2.4.2. Responsibilities and competences of the process managers

The process manager, on the instructions of his/her board, directorate or privacy & security coordinator, carries out activities for the privacy-proofing of the processes within that faculty or service unit. The process manager also records the processing of personal data and registers the data in the appropriate register. The process manager thus implements the responsibility of their board or directorate at the level of the process or processes they manage.

2.4.3. Responsibilities and competences of researchers

The researcher is the process manager of his/her research. The researcher thus has an independent responsibility to privacy-proof that research. In fulfilling this responsibility, the ethics committees have a role to play. The 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 Research Data Office.

2.4.4. 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, codes of conduct 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.

2.5. Responsibilities and competences of the DPO

The DPO is responsible for supervising compliance with the privacy laws and regulations and the privacy policy. Within the UG, the DPO has, as a minimum, the duties, responsibilities and competences that are assigned to him/her 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 itself and to the processing activities 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 provides solicited and unsolicited advice to all administrative layers of the UG. The DPO is empowered to perform tasks and to keep his/her expertise up to date. The DPO reports directly to the Board of the University. The DPO supports the Board of the University in rendering account externally, both to supervisors and to the data subjects. 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. Responsibilities and competences of the IT lawyer and Security Manager

2.6.1. Responsibilities and competences of the IT lawyer

The IT lawyer gives actual substance to the implementation of the privacy laws and regulations within the UG. The IT lawyer supervises DPIAs, draws up processor agreements and develops privacy statements. The IT lawyer supports all staff members and in particular the privacy & security coordinators, process managers, researchers and the DPO in performing their duties. The IT lawyer advises on the further elaboration of this privacy policy. The IT lawyer continuously coordinates his/her work with the DPO and the Security Manager.

2.6.2. Responsibilities and competences of the Security Manager

The Security Manager supports the UG in taking appropriate technological and organizational measures to protect personal data against unauthorised access and unlawful processing. To that end, the Security Manager gives advice to the privacy & security coordinators, DPO and IT lawyer. The Security Manager, or an expert designated by him/her, participates in DPIAs that are performed under the responsibility of the UG.

2.7. Responsibilities and competences of the 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. Work programme for privacy-proofness and policy evaluation

The Board of the University establishes an annual work programme, linked to a 'maturity model' for privacy-proofness, for the furtherance of the privacy-proofness of the organization and the application of this privacy policy in accordance with a *Plan-Do-Check-Act* cycle. This is done partly on the basis of the reports from the faculty boards and service directorates as referred to in Section 2.2 and the recommendations issued by the DPO, IT lawyer and/or the Security Manager. The DPO, IT lawyer and Security Manager prepare a draft of this work programme for the Board of the University, including a budget proposal.

The work programme will first be adopted in 2019. The Board of the University will decide annually on any adjustments to this privacy policy, with due observance of the reports of the faculty boards and service directorates and the recommendations of the DPO.

3.2. PDCA cycle to make processes privacy-proof

The Faculty Board and the service directorates are responsible for implementing a *Plan-Do-Check-Act* cycle that enables them to make and keep the processes within their faculty or service unit privacy-proof. In that context, they determine how and when the faculty board or service directorate implements the tasks and responsibilities described in section 2.2. They also provide a periodic evaluation of the actions taken and determine which measures must be taken to further optimise the privacy-proofness of their faculty or service unit.

The IT lawyer, DPO and Security Manager coordinate efforts to streamline similar and overlapping processes between faculties and service units.

3.3. Measuring privacy-proofness, audits

The Board of the University is responsible for the implementation of mechanisms throughout the organization and at the level of service units and faculties by means of which the privacy-proofness of the organization or a faculty or service unit can be assessed and measured. In the annual work programme for privacy-proofness, the Board of the University, in consultation with the DPO, establishes the mechanisms and, in consultation with the faculty boards and service directorates, makes sure they are implemented. At least once a year, the DPO reports the results to the Board of the University and evaluates them together with the Board of the University.

In the annual work programme, the Board of the University determines when the privacy-proofness of the organization or parts of the organization must be assessed by means of an audit by an internal or external expert.

3.4. Privacy by Design, 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. 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 stipulates when the support of the Department of General Administrative and Legal Affairs (ABJZ) is required. Faculty boards and service directorates are responsible for compliance

with this protocol. When Privacy by Design has been applied or a DPIA has been carried out, this will be recorded in the register referred to in Section 3.6. The information from DPIA reports will be used for preparing the work programme referred to in Section 3.1.

3.5. 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. In the annual work programme, the Board of the University will decide to which codes of conduct the UG will adhere. The DPO may advise the UG to conform with codes of conduct.

3.6. 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 the privacy laws and regulations, but is also an instrument to achieve privacy-proofness and to be accountable for this. ABJZ, in consultation with the 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.

3.7. 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 unauthorised access. The measures are both technical and organisational 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 directorates are responsible for this. They are supported in this by the privacy & security coordinator, the Security Manager and the DPO or IT lawyer.

3.8. 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. The notifications are handled according to the Protocol for Mandatory Notification of Data Breaches of the UG. The protocol is evaluated on an annual basis by ABJZ and is updated in consultation with the Security Manager and the DPO. Reported data breaches are recorded in the register referred to in Section 3.6.

3.9. 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. In the latter case, the provision of data to a third party will always be coordinated with the DPO or IT lawyer. The DPO and the IT lawyer will assess the legality of the 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, the IT lawyer 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 after approval by ABJZ. The agreements are signed by or on behalf of the Board of the University. With multi-institutional collaborations on agreements concerning the processing of personal data, the IT lawyer and the DPO will play a coordinating role.

3.10. 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 IT lawyer will always give instructions for arranging these safeguards.

3.11. Transparency and accountability

3.11.1. 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 person concerned 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 Board and the service directorates are responsible for ensuring that this specific privacy statement is drafted and submitted. They coordinate this with the DPO or IT lawyer. In the case of scientific 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 approval. Complementary privacy statements are registered with ABJZ.

3.11.2. Rights of the data subject

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. For this purpose, a *Central Privacy Desk* has been set up 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.

3.11.3. Accountability to privacy supervisors

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

3.12. 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 privacy portal has been set up on the UG's intranet. The privacy portal will contain information about privacy laws and regulations, work instructions and model contracts. The UG will make information publicly available 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 the DPO and the IT lawyer.

In the event of a privacy incident or other privacy-related PR issue, the Board of the University will be accountable to those concerned, 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.

3.13. Raising awareness and training

The UG works continuously to raise staff awareness of privacy-proofness. For example, codes of conduct 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.

3.14. Nature of this privacy policy

This privacy policy provides general guidelines for achieving privacy-proofness, 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 which conditions must be met for privacy-proofness.

3.15. Implementation and further elaboration of privacy policy

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

The Board of the University may issue University-wide protocols and codes of conduct that prescribe how staff members, process managers or privacy & security coordinators must act when handling personal data. A faculty board or service directorate may do this for its faculty or service unit. After assessment by the DPO and the IT lawyer, these protocols and codes of conduct must be approved by the Board of the University before they are declared applicable.

4. Definitions of terms used

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

- ABJZ: the Department of General Administrative and Legal Affairs of the UG
- GDPR: the General Data Protection Regulation
- Person concerned: the natural person whose personal data are being processed
- 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

- IT lawyer: a lawyer from ABJZ who deals with issues relating to privacy laws and regulations
- Personal data: all data relating to a natural person and identifying this person directly or indirectly
- Privacy-proofness: 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 directorate to coordinate the privacy-proofness of a faculty, service unit or department thereof
- Privacy statement: the statement, form for informed consent or any other document informing the person concerned 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: the UG staff member who bears the responsibility within a faculty or service unit where a process or several related processes are performed
- Privacy policy: this general policy on the protection of personal data at the UG
- Privacy impact: the adverse consequences of a process or processing for the careful and proper handling of personal data and for the protection of the privacy of a data subject
- Research Data Office: 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;
- UG: University of Groningen
- Security Manager: the staff member of the Center for Information Technology of the UG who is responsible for the development of strategy and policy aimed at information security and the translation of policy into implementation plans
- Processing: 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 that processes personal data on behalf of the UG.