

GENERAL POLICY ON THE PROTECTION OF PERSONAL DATA

UNIVERSITY OF GRONINGEN

Version 4 – 26 May 2026 - adopted by the Board of the University

Author: J.W. Oordt, LL.M. – Chief Privacy Officer

Contents

1. Definitions of terms used.....	4
2. Principles.....	5
2.1. Introduction	5
2.2. Privacy vision of the University of Groningen	5
2.3. Purpose	5
2.4. Target group	6
2.5. Scope.....	6
2.6. Interrelationships with and relationship to other policy areas and policy documents	6
2.7. Legal framework	6
2.8. Effective date and maintenance	7
3. Privacy governance	7
3.1. Three lines model, integration of Privacy & Security (P&S).....	7
3.2. Responsibilities and powers of faculty boards / service management teams	8
3.3. Responsibilities and powers of the Board of the University	9
3.4. Responsibilities and powers of privacy & security coordinators, the P&S Guild and staff	9
3.4.1. General	9
3.4.2. Responsibilities and powers of privacy & security coordinators	9
3.4.3. Responsibilities and powers of the P&S Guild	9
3.4.4. Responsibilities and powers of staff	10
3.4.5. Responsibilities and powers of researchers	10
3.4.6. Responsibilities and powers of students	10
3.5. Responsibilities and powers of the CPO, AJZ and CISO	10
3.5.1. Responsibilities and powers of the CPO	10
3.5.2. Responsibilities and powers of AJZ.....	10
3.5.3. Responsibilities and powers of the CISO	11
3.6. Responsibilities and powers of the Data Protection Officer and IT auditor	11
3.6.1. Responsibilities and powers of the DPO	11
3.6.2. Responsibilities and powers of the IT auditor	12
3.7. Responsibilities and powers of the Privacy, Security and Information Management Committee	12
3.8. Responsibilities and powers of co-participation bodies	12
4. Implementation of privacy policy	12
4.1. Work programme on privacy maturity of the Board of the University, policy evaluation, further privacy policy, protocols	12
4.2. PDCA cycle for data protection in faculties and services.....	13
4.3. Privacy by Design & by Default, DPIA's	13
4.4. Codes of conduct and certifications	13

4.5.	Register of processing activities	14
4.6.	Information security	14
4.7.	Privacy incidents, data breaches	14
4.8.	Processing of the UG's personal data by or in conjunction with third parties	14
4.9.	Transfer of personal data outside the EEA.....	15
4.10.	Transparency and accountability	15
4.10.1.	Privacy statement	15
4.10.2.	Rights of the data subject	15
4.10.3.	Accountability to data protection authorities	15
4.11.	Communication and PR	15
4.12.	Awareness and training	16
4.13.	Nature of this privacy policy	16
5.	Protocols and further privacy policies	16

1. Definitions of terms used

The terms used in this privacy policy are defined as follows:

- AJZ: the General and Legal Affairs Department of the UG;
- GDPR: the General Data Protection Regulation;
- Data subject: the natural person whose personal data is being processed;
- CISO: the Chief Information Security Officer of the UG;
- CPO: the Chief Privacy Officer of the UG;
- Privacy, Security & Information Management Committee: the strategic committee that advises the BoU on the application of this privacy policy in relation to the UG's strategic objectives;
- BoU: the Board of the University of Groningen;
- Digital Competence Centre (DCC): a collaboration between the University Library and the Centre for Information Technology at the UG to support researchers and research institutes with data management;
- DPIA: Data Protection Impact Assessment, an assessment of the privacy impact of a process or system in which personal data is processed;
- DPO: the UG's Data Protection Officer;
- GRC tool: the digital environment for Governance, Risk & Compliance, in which P&S risks and mitigating measures are recorded and monitored;
- P&S Guild: the partnership and consultative body of P&S coordinators;
- Personal data: all data relating to a natural person and identifying that person directly or indirectly;
- Privacy maturity: compliance with privacy legislation and regulations and ensuring the careful and proper handling of personal data;
- Privacy & Security Coordinator: the UG staff member appointed by a faculty board or the management of a service to coordinate the privacy maturity of a faculty, service or a division thereof;
- Privacy statement: the statement, informed consent form or other document in which the data subject is informed about the processing of their personal data by the UG;
- Privacy legislation and regulations: all national or international legislation and regulations applicable to the UG and imposing conditions regarding the processing of personal data, including the GDPR;
- Privacy policy: this general policy on the protection of personal data;
- Privacy impact: the adverse consequences of a process or processing for the careful and proper handling of personal data and for the protection of a data subject's privacy;
- UG: University of Groningen;
- Processing, to process: any operation or set of operations performed on personal data, such as viewing, sharing, modifying, copying, storing and destroying;
- Processor: any natural or legal person or organisation that processes personal data on behalf of the UG.

2. Principles

2.1. Introduction

Due to increasing digitalisation and growing awareness of the importance of protecting an individual's privacy, privacy has become an increasingly relevant topic. Part of the right to protection of privacy is the right to protection of personal data. This gives rise to an obligation for the UG to handle the personal data of students, research subjects, staff and anyone else whose personal data it processes with due care. The Board of the University of Groningen (hereinafter: the BoU) wishes this obligation to be applied throughout the university. To this end, the BoU has adopted this policy (hereinafter: the Privacy Policy), which outlines the vision, principles and governance regarding the protection of personal data.

2.2. Privacy vision of the University of Groningen

The UG's mission is to generate, share and preserve knowledge and information, with the aim of contributing to the resolution of societal and scientific challenges. In this way, the UG aims to make a significant contribution to society. The UG adheres to a privacy vision that is consistent with this mission. This vision is as follows.

Every student, every staff member, every research subject and everyone else who is in any way connected to the UG must be able to trust that their personal data is processed lawfully by the UG and is adequately protected. At all times, the UG handles the personal data it processes with care and due diligence. By complying with applicable privacy laws and regulations, the UG offers a consistent and high level of protection for the rights and freedoms of individuals ('privacy maturity').

The UG is therefore transparent about what it does with personal data and takes responsibility, even when mistakes are made. The UG enables individuals to access and correct their data. Their questions and any complaints are taken seriously and dealt with appropriately.

Within this framework, excellence in education and research is facilitated and achieved as much as possible. Privacy maturity pays off by making a positive contribution to the UG's mission.

2.3. Purpose

The objective of this privacy policy is:

- To ensure the careful, proper and secure handling of the personal data processed by the UG, in accordance with applicable privacy laws and regulations, in such a way that the rights and freedoms of individuals are respected;
- To establish the frameworks within which this policy is implemented;
- To prevent privacy incidents and, in case they do occur, to limit the damage to individuals and the organisation;
- Implementing measures and mechanisms that optimise the UG's privacy maturity;
- To facilitate and empower all UG staff to contribute to the organisation's privacy maturity;
- Enabling the BoU to report with confidence to data subjects and authorities.

2.4. Target group

The target group for the obligations set out in this policy comprises all staff and students of the UG. The responsibilities, duties and powers that staff and students have with regard to the protection of personal data are set out in more detail in this privacy policy. In the interests of transparency regarding the processing of personal data, the policy is published on the UG's public website.

2.5. Scope

This privacy policy applies to the processing of personal data. Personal data refers to any information relating to a natural person that directly or indirectly identifies that person. Processing refers to any operation or set of operations performed on personal data, such as viewing, sharing, modifying, copying, storing and destroying. The policy covers the entire lifecycle of personal data, from the moment of collection or creation of personal data until its deletion or destruction. The policy applies to both automated and non-automated processing.

The policy applies to the entire university. It covers all university processes involving the processing of personal data, both in the context of teaching and research and in the context of the operational activities that facilitate and support these primary tasks. Where the processing of personal data is carried out by a third party on assignment from the UG, jointly with the UG or otherwise by or on behalf of the university, this policy also applies.

2.6. Interrelationships with and relationship to other policy areas and policy documents

This privacy policy overlaps with other policy areas within the UG, such as information security, *Artificial Intelligence* and archiving. This privacy policy has been aligned as much as possible with the policies drawn up for those areas. However, it is possible that other policies place different emphases with regard to the protection of personal data. These must always be assessed in the light of this privacy policy.

2.7. Legal framework

The legal framework for this privacy policy is primarily formed by the General Data Protection Regulation (GDPR). In addition, there is national implementing legislation (e.g. the Dutch GDPR Implementation Act) and legislation setting out rules for specific forms of personal data processing. Furthermore, legislation applies to the UG that may provide specific instructions regarding processing, such as retention obligations or anonymisation obligations (e.g. the Public Records Act and the Open Government Act). In addition, where applicable, other legislation to which the UG must adhere (e.g. the Higher Education and Research Act, the General Administrative Law Act and the AI Regulation) forms part of the legal framework. However, defining the relationship between the various pieces of legislation in more detail in this policy would go too far. This 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 body (e.g. the Dutch Data Protection Authority or the European Commission). This also applies to opinions issued by the Data Protection Officer (hereinafter: DPO). Codes of conduct may also be drawn up by umbrella organisations such as the UNL (e.g. code of conduct for the use of personal data in scientific research) or by the UG itself, to which the university is committed.

2.8. Effective date and maintenance

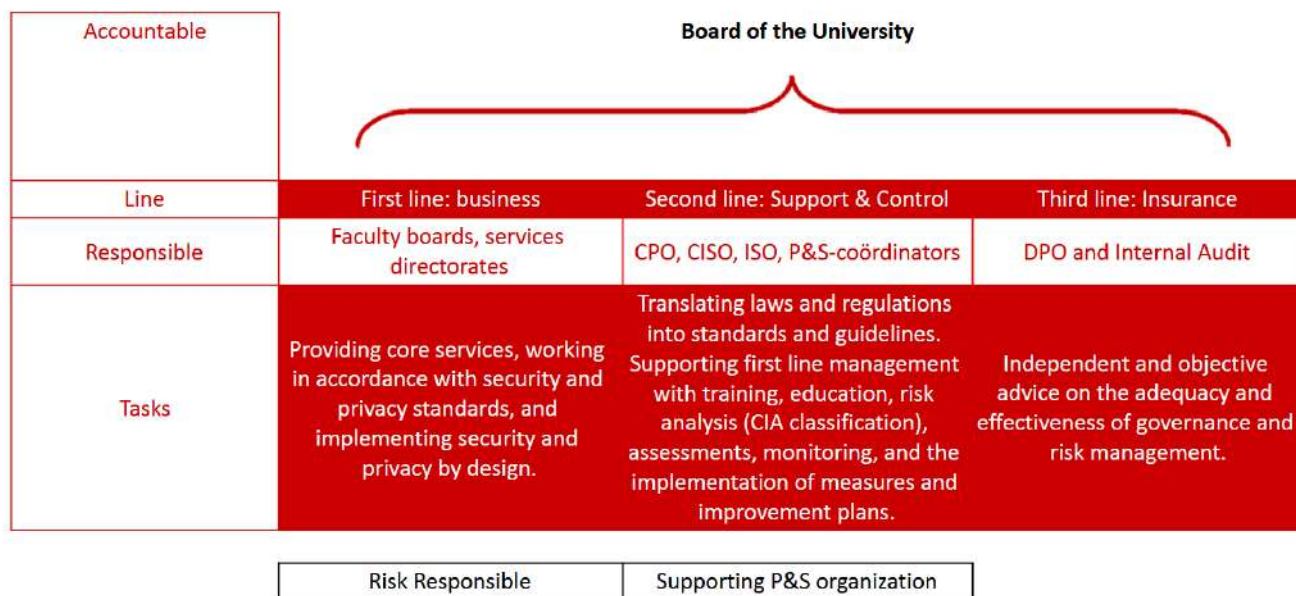
The first version of this privacy policy was adopted on 4 June 2018 by the BoU and has been in force since that date. The policy will be updated and supplemented at least once every two years. Amendments come into force following approval by the BoU.

3. Privacy governance

3.1. Three lines model, integration of Privacy & Security (P&S)

Privacy governance is organised in conjunction with information security. *Privacy & Security* (P&S) are therefore very closely intertwined at the UG, not only in terms of content but also in terms of organisation. Governance is structured according to the so-called ‘three lines model’¹. This model describes the various roles, responsibilities and relationships regarding the formulation of policy and measures, the implementation of measures, and the assessment and monitoring of these measures for P&S. The model is shown schematically in Figure 1.

Figure 1. Governance structure Privacy & Security



1st line

The ‘three lines’ model is based on the principle that the faculty boards and management teams of services (‘the business’) are responsible for organising their own processes. Privacy and information security form an integral part of this. The boards and management teams are supported in this by P&S coordinators.

2nd line

The CISO and CPO submit proposals to the Board of the University regarding policy and measures in the field of information security and privacy. They support and advise the 1st line and assess whether it is fulfilling its responsibility with regard to information security and data protection.

¹ The Institute of Internal Auditors (IIA) Three Lines Model, [Three Lines Model Updated - ENG \(iaa.nl\)](https://www.iaa.nl/en/three-lines-model).

3rd line

The 3rd line acts as an independent check on the interaction between the first and second lines and provides an objective, independent assessment thereof, including suggestions for improvement. The audit may be carried out by the Data Protection Officer, an internal IT auditor and/or an external auditor.

A further elaboration of these responsibilities in terms of scope, tasks and powers is provided in the remainder of this policy. At all times, the board or management to which a P&S officer reports shall involve this person in a timely manner and provide the resources and time necessary to perform the role properly.

3.2. Responsibilities and powers of faculty boards / service management teams

The faculty boards and the management teams of the UG's services are responsible for ensuring that their faculty or service complies with privacy legislation and this privacy policy. The board or management team has the following tasks and responsibilities:

- Ensuring awareness of the importance of privacy maturity and the protection of personal data within the faculty or service;
- Identifying all processing of personal data within their faculty or service, recording this processing in the designated register and keeping these records up to date;
- Identifying the risks to the protection of personal data arising from the processing activities of the organisational unit and assessing and mitigating these risks;
- Ensuring that the processing of personal data by the faculty or service complies with privacy legislation and regulations;
- Ensuring that a DPIA is carried out where required under data protection legislation and regulations and/or UG policy;
- Based on a DPIA or other risk analysis, establishing appropriate safeguards for the protection of personal data and implementing appropriate technical and organisational measures;
- Monitoring and improving the privacy maturity of their faculty or service;
- Reporting (suspected) data breaches and privacy incidents within the faculties or services in a timely and comprehensive manner;
- Coordinating with other faculties and services within the P&S Guild regarding the application of this policy, so as to avoid duplication of effort;
- Informing the faculty council or employee council at least once a year on the state of play regarding the above activities.

The Board or Management translates the above responsibilities for the areas of education, operational management and scientific research into specific measures and actions. Data protection risks, measures and actions are recorded in the UG's GRC *tool*, in accordance with the P&S risk management policy and the P&S risks and measures protocol. This facilitates control and visibility of risks, ensures a cycle of improvement and promotes cooperation between faculties and services.

Privacy is a separate area of focus for a faculty board or management team. If a faculty board or management team consists of several people, it is determined which board member is responsible for privacy. The board or management team ensures sufficient staffing to carry out the above responsibilities and tasks and appoints at least one privacy & security coordinator to coordinate the application of privacy legislation and regulations and this privacy policy within their faculty or service.

The faculty boards and management teams of services are accountable to the BoU for the fulfilment of the above responsibilities. Annually, the CPO and CISO, on behalf of the BoU, assess whether the faculty or service complies with the requirements of this privacy policy and the P&S risk management policy.

3.3. Responsibilities and powers of the Board of the University

The BoU bears ultimate responsibility for the management of the University's data files and the privacy maturity of the UG. The BoU represents the UG in dealings with external supervisory authorities, data subjects and third parties. Furthermore, the BoU informs the University Council and the Supervisory Board where necessary about developments in this area. The BoU may be supported by the Data Protection Officer (DPO), the Chief Privacy Officer (CPO) and the Chief Information Security Officer (CISO) when rendering account and providing information. The BoU ensures that the DPO is involved in a timely and sufficient manner in matters concerning the protection of personal data.

Every two years, based on a proposal from the CPO, the BoU determines how the UG should further develop in terms of privacy maturity. In doing so, the BoU takes into account the recommendations issued by the Data Protection Officer. Any deviation from these recommendations must be duly justified. The BoU facilitates the UG's bodies and staff in complying with privacy legislation and regulations and makes resources and support available for this purpose. When a faculty board or the management of a service fails to comply with privacy legislation and regulations or this privacy policy, the BoU shall take reasonable measures or impose sanctions to remedy the situation.

3.4. Responsibilities and powers of privacy & security coordinators, the P&S Guild and staff

3.4.1. General

Privacy & security coordinators, researchers and other staff members work under the responsibility of the faculty board or the management of the service to which they belong.

3.4.2. Responsibilities and powers of privacy & security coordinators

The privacy & security coordinator is the first point of contact for privacy-related queries from staff of the faculty or service. The coordinator also maps out the processing of personal data and records it in the designated register. The privacy & security coordinator supports colleagues in the faculties or services in carrying out DPIA's and in drafting and assessing privacy agreements. The privacy & security coordinator reports to their respective board or management.

3.4.3. Responsibilities and powers of the P&S Guild

The Privacy & Security Guild (P&S Guild) is the collaborative body and consultative forum for the P&S coordinators at the UG. The P&S Guild ensures that faculties and services collaborate wherever possible on addressing P&S issues and mitigating P&S risks. The P&S Guild prioritises the tackling of these issues and cross-faculty and cross-service risks, and ensures solutions that can be applied across the university. When developing and implementing measures, the P&S Guild takes the practical, day-to-day realities of staff and students into account as much as possible. The P&S Guild organises university-wide awareness campaigns to enhance the knowledge and skills of staff and students. The CPO and the CISO chair the P&S Guild's meetings and oversee the implementation of the above tasks.

3.4.4. Responsibilities and powers of staff

All staff members at the UG have a responsibility to handle the personal data they process with care. They shall familiarise themselves with the relevant policies, protocols and instructions and comply with them. Where necessary and possible, they shall support the P&S organisation with their knowledge and expertise. Should they become aware of any potential privacy incidents, they shall report these as soon as possible to the designated reporting points or the Data Protection Officer.

3.4.5. Responsibilities and powers of researchers

The researcher bears independent responsibility for the privacy maturity of their research. The ethics committees play a role in the fulfilment of this responsibility. On behalf of the faculty board, they oversee the assessment of the research against ethical and legal requirements. The researcher complies with privacy legislation and regulations, (ethical) guidelines and codes of conduct in the field, and faculty policy. In addition to the regular support provided within the faculty, support is provided by the Digital Competence Centre (hereinafter: DCC).

3.4.6. Responsibilities and powers of students

It may happen that students at the UG gain access to personal data as part of their studies. Students shall handle personal data with care and comply with university policy and the instructions they receive from their teachers and supervisors. Faculties are responsible for guiding students in the use of personal data.

3.5. Responsibilities and powers of the CPO, AJZ and CISO

3.5.1. Responsibilities and powers of the CPO

The Chief Privacy Officer (CPO) is responsible for developing and implementing the university's privacy policy, including guidelines and procedures for protecting the personal data of students, staff, research subjects and other individuals. The CPO ensures that the faculties and services act in accordance with this policy and that the resulting measures are applied. The CPO advises faculties and services on identifying and managing risks and provides substantive support to the privacy and security coordinators. The CPO advises the BoU on the follow-up to the Data Protection Officer's annual report and the implementation of their recommendations. The CPO, together with the CISO, leads the P&S Guild. Every two years, in collaboration with the P&S Guild, the CPO draws up a work programme outlining how the UG will achieve further growth in privacy maturity.

The CPO advises on complex privacy matters, initiates risk analyses and privacy audits, organises awareness programmes, and advises the Board and management. The CPO ensures an overview of and oversight over the privacy risks present within the university. The CPO reports on their activities to the Privacy, Security & Information Management Committee and is employed by the AJZ department.

3.5.2. Responsibilities and powers of AJZ

AJZ advises faculties and services on the application of privacy legislation and regulations within the UG. AJZ supports faculty boards, service management teams and their privacy and security coordinators in drawing up DPIA's, (privacy) agreements and privacy statements. AJZ supports the Data Protection Officer (DPO) in the performance of their duties. AJZ advises on the further elaboration of this privacy policy. AJZ employs a coordinator for

awareness and training activities in the field of privacy and security. This officer supports the privacy and security coordinators, the Privacy and Security Guild, the CPO and the CISO in planning and carrying out activities that enhance the knowledge and skills of staff and students in the field of privacy and security.

AJZ draws up model agreements that can be used by staff of the UG to enter into agreements with third parties for the careful and secure exchange and processing of personal data. Entering into the actual agreements must always take place in accordance with AJZ's instructions. Signing is carried out by or on behalf of the BoU. AJZ ensures a process is in place to monitor compliance with the agreements made.

AJZ continuously coordinates its privacy-related activities with the Data Protection Officer (DPO), the Chief Privacy Officer (CPO) and the Chief Information Security Officer (CISO).

3.5.3. Responsibilities and powers of the CISO

The CISO is responsible for developing and implementing an information security programme, comprising policies, measures and procedures designed to protect the UG's information systems against internal and external threats. The CISO monitors the functioning of the Information Security Management System (ISMS) and oversees compliance with the information security policy and the resulting measures throughout the organisation, advises on complex security issues, initiates risk analyses and security audits, organises security awareness programmes, and advises the Board of the University, faculty boards and service management teams.

The CISO advises the UG Board, where necessary in conjunction with the CPO, the Data Protection Officer (DPO) and/or the IT auditor, on the security risks faced by the faculties and services in relation to information security and privacy protection. The CISO provides substantive guidance to the Security Team and the Security Operations Centre (SOC). In addition, the CISO chairs the UG's Cybersecurity Incident Response Team (CSIRT).

3.6. Responsibilities and powers of the Data Protection Officer and IT auditor

3.6.1. Responsibilities and powers of the DPO

The DPO is responsible for providing solicited and unsolicited advice to the BoU on, and for monitoring compliance with, privacy legislation and regulations and the privacy policy. Within the UG, the DPO has at least the duties, responsibilities and powers conferred on the DPO by privacy legislation and regulations.

The DPO has access to all information held by the UG relating to the processing of personal data – both to the personal data itself and to the processing activities and the systems used to carry out those activities. The BoU may stipulate that, before access is granted to certain information, prior notification must be given to the BoU. The DPO supervises the register of processing activities.

The DPO is enabled to carry out their duties and maintain their expertise and, in line with Article 38 of the GDPR, is provided with the necessary resources. The DPO acts as an adviser to the BoU and reports directly to the BoU. The DPO publishes an annual report on the protection of personal data within the UG, including the current status regarding privacy maturity. The report is made available to the BoU and the Supervisory Board. The report is sent to the University Council for information.

The DPO supports the BoU in its external accountability, both to supervisory authorities and to data subjects. To this end, the DPO maintains contact with the supervisory authorities. The DPO makes recommendations aimed at further optimising the implementation of privacy policy.

3.6.2. Responsibilities and powers of the IT auditor

The internal IT auditor monitors risk management and the effectiveness of risk-mitigating measures in relation to university processes and information systems. As part of a BoU assignment, the UG's IT auditor assesses the design, existence and operation of the university's privacy policy and measures that mitigate risks to the protection of personal data. The IT auditor sets out these activities in a university audit plan. The IT auditor reports on their activities to the Privacy, Security and Information Management Committee.

3.7. Responsibilities and powers of the Privacy, Security and Information Management Committee

The Privacy, Security and Information Management Committee advises the BoU on the development of university-wide policies and work programmes in the field of privacy, information security and information management. The committee ensures that privacy, information security and information management are aligned with the university's strategic objectives. The committee oversees the application of the ownership model, which determines responsibility for processes, systems, data and risks. Changes to the privacy policy are always submitted to this committee before being presented to the BoU for adoption. The CISO and CPO report to the committee on a quarterly basis regarding the progress of the roll-out of their work programmes. The committee consists of a member of the BoU (who also chairs the committee), two members of the Management Council, a member of the Committee of Deans, the directors of University Services and the Centre for Information Technology, the CISO and the CPO. The IT auditor and the Data Protection Officer are advisory members.

3.8. Responsibilities and powers of co-participation bodies

To the extent required by law or internal policy, the UG's co-participation bodies are empowered to exercise their powers regarding the manner in which the UG implements privacy legislation and regulations. The powers of the University Council in the field of privacy and the protection of personal data are laid down in the University Council Regulations.

4. Implementation of privacy policy

4.1. Work programme on privacy maturity of the Board of the University, policy evaluation, further privacy policy, protocols

The UG uses a standard model to determine privacy maturity. This is SURF's 'Privacy Assessment Framework'.² The UG has set itself the target of operating at a minimum average maturity level of 3.0 according to this model (on a scale of 0–5). When applying the model, the structure and culture of the organisation are taken into account. Every two years, in response to the assessment of the university's current maturity level, the Board of the University sets out in a work programme what needs to be done to achieve and maintain the desired level. The work programme is prepared by the CPO in consultation with the P&S

² See: <https://pec.surf.nl/surfaudit-toetsingskader-privacy/>.

Guild. The CPO incorporates its implementation into the university's Plan-Do-Check-Act cycle for data protection and ensures that the work programme is embedded in the activities of the P&S Guild of faculties and services.

This privacy policy is reviewed and updated at least once every two years. The Board of the University may adopt further privacy policies for specific processing operations where necessary.³ The Privacy, Security & Information Committee establishes protocols to facilitate compliance with the obligations under the GDPR, including a process description and working instructions. These protocols are developed and managed by the CPO, where necessary in collaboration with the CISO.

4.2. PDCA cycle for data protection in faculties and services

The faculty boards and the management teams of the services are responsible for implementing a *Plan Do Check Act* cycle to ensure that the processes within their faculty or service are made and kept privacy-mature and compliant. In this context, they determine how and when the board or management will carry out the tasks and responsibilities described in section 2.2. They do so by implementing the risk management policy and continuously identifying and mitigating privacy risks through concrete actions and measures relating to processes and systems. This is described in more detail in the P&S risks and measures protocol. The activities of the board or management are assessed annually by the university's Data Protection Officer (DPO), Chief Privacy Officer (CPO), IT auditor and Chief Information Security Officer (CISO). The structure and functioning of the P&S organisation of the faculty or service are also assessed. The faculty board or management receives feedback on the assessment.

4.3. Privacy by Design & by Default, DPIA's

Innovative research projects and new processes within the UG, as well as the systems that support these processes, are designed to minimise the impact on privacy while achieving the legitimate purposes of these processes. *Privacy by design* and *privacy by default* are integral to the process of procuring, developing and implementing information systems. Privacy by design involves embedding the principles of the GDPR into processes and systems within which personal data is processed, right from the design phase. Privacy by default involves configuring the default settings of a system or process in such a way that the impact on the data subject's privacy is minimised.

Where necessary, a *Data Protection Impact Assessment (DPIA)* is carried out. The UG has a protocol that determines when this is mandatory and that encourages the sharing of insights from the DPIAs. The protocol complies at a minimum with the requirements of privacy legislation and regulations and specifies when a supporting role from AJZ is required. Faculty boards and service management teams are responsible for compliance with this protocol. Where a DPIA has been carried out, this is recorded in the register referred to in section 3.5. A DPIA is always shared with the UG Data Protection Officer (DPO) for the purpose of obtaining advice.

4.4. Codes of conduct and certifications

Where possible and reasonable, the UG complies with codes of conduct and certification requirements that promote the careful and proper handling of personal data. The BoU

³ Consider, for example, the CCTV policy.

decides in the biennial work programme which codes of conduct the UG will comply with. The DPO may advise the UG to comply with codes of conduct.

4.5. Register of processing activities

All processing of personal data by or on behalf of the UG is recorded in a central, publicly available register⁴ managed by the CPO. This register meets the requirements of privacy legislation and regulations, but also serves as a tool for achieving privacy maturity and being able to account for it. The CPO, in consultation with the Data Protection Officer (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 a data controller and as a data processor within the meaning of privacy legislation and regulations. The CPO assesses the registered processing operations and advises the faculties and services on the risks associated with a processing operation.

4.6. Information security

The UG's information security policy and the associated baseline of measures provide for appropriate protection of personal data against unlawful processing and unauthorised access. The measures may be technical or organisational. The information security policy applies to all processing of personal data by the UG, whether or not involving external parties (processors) or jointly with another responsible party. Personal data is classified as at least 'confidential' within the meaning of the information security policy. For each process in which personal data is processed, an assessment is made as to whether this level is appropriate. Faculty boards and service management teams are responsible for this.

4.7. Privacy incidents, data breaches

(Suspected) data breaches and other (security) incidents that compromise the protection of personal data can be reported to a dedicated *data breach reporting centre* for which the CPO is responsible. Reports are handled in accordance with the UG's Data Breach Reporting Protocol. The protocol is reviewed annually by the CPO, the CISO and the DPO. Reported data breaches are recorded in a non-public register.

4.8. Processing of the UG's personal data by or in conjunction with third parties

The UG may outsource the processing of personal data to third parties, carry out such processing in collaboration with third parties, or provide personal data to third parties. AJZ assists in assessing the lawfulness of such activities. Where processing is carried out by a third party, written agreements are made with that party to ensure that personal data is handled with due care and in an appropriate manner. The agreements comply with the requirements of privacy legislation and regulations, including Articles 26 and 28 of the GDPR.

⁴ See: <https://www.rug.nl/about-ug/policy-and-strategy/privacy-and-security-at-the-ug/processing-register/>.

4.9. Transfer of personal data outside the EEA

The processing of personal data outside the European Economic Area (EEA) is only possible if appropriate safeguards have been put in place to protect the personal data in accordance with privacy laws and regulations. Prior to such processing, the DPO or AJZ will always provide guidance on implementing these safeguards.

4.10. Transparency and accountability

4.10.1. Privacy statement

Data subjects are informed fully, in a timely manner and in understandable language about the processing of their personal data by the UG. There is a UG-wide privacy statement to which the data subject is referred prior to the processing of their personal data. This is managed by the CPO.

Where necessary, data subjects must be provided with a specific privacy statement for specific processing operations, which supplements and refers to the UG-wide privacy statement. The faculty board and the management teams of the services are responsible for ensuring that this specific privacy statement is drawn up and presented. They coordinate this with the relevant privacy and security coordinator. In the case of scientific research, this is done in consultation with the ethics committee. Such a supplementary privacy statement is drawn up in any event when the data is processed on the basis of the data subject's consent. Supplementary privacy statements are registered with AJZ.

4.10.2. Rights of the data subject

All requests, queries and complaints from a data subject regarding the processing of their personal data by the UG are assessed and dealt with in a timely, careful and proper manner. A *Central Privacy Desk* has been set up at AJZ for this purpose. There is a protocol for handling requests received by the desk. This describes how requests from data subjects are dealt with in accordance with privacy legislation and regulations (for example, a request for access or a request for the erasure of their personal data). The CPO manages this protocol. Data subjects are informed of their rights and of the Central Privacy Desk in every privacy statement.

4.10.3. Accountability to data protection authorities

Under the GDPR, the Data Protection Officer (DPO) acts as the contact person for the Dutch Data Protection Authority. This does not affect the BoU's accountability to the competent national and international privacy regulators and the Supervisory Board. The BoU is responsible for providing full information and demonstrating the UG's privacy maturity.

4.11. Communication and PR

All staff members are informed about this privacy policy and the duties and responsibilities they have under it. To this end, a webpage has been set up on the UG's intranet. The website contains information on privacy legislation and regulations, as well as work instructions. The UG also publishes information on its public website regarding the handling of personal data and the university's privacy vision. The information is drafted and maintained by the Communications Department of the University Services service division of the UG, in collaboration with AJZ.

In the event of a privacy incident or other potential privacy-related PR issues, the BoU is accountable to those affected, regulators and other stakeholders. The Data Protection Officer may, always in consultation with the BoU, provide an account on behalf of the BoU.

4.12. Awareness and training

The UG is constantly working to raise awareness regarding privacy maturity. All UG staff undertake training to familiarise themselves with the relevant aspects of privacy legislation and regulations, as well as work instructions for the careful handling of personal data.

4.13. 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 a specific processing activity. For each processing activity, a conscious and separate assessment must be carried out to determine how it can be brought into compliance with legislation, regulations and this policy. Where necessary, this will be enshrined in further privacy policies.

5. Protocols and further privacy policies

This general privacy policy is further elaborated in protocols and supplementary privacy policies. The protocols describe work processes with tasks, responsibilities and authorities for handling data breaches, privacy requests, DPIA's and P&S risks. Further privacy policies describe the objectives, responsibilities and further standards of care for specific processing operations involving high risks to the protection of personal data, such as camera surveillance. These documents ensure that the fulfilment of the obligations under the GDPR is properly embedded within the organisation. The Board of the University has adopted the following protocols and further privacy policies:

Protocols	Detailed privacy policy
Protocol on the obligation to report data breaches	P&S Risk Management Policy (also part of the UG's information security policy, adopted in 2024)
DPIA Protocol and DPIA Protocol in Research	Camera Surveillance Policy (adopted in 2025)
Central Privacy Helpdesk Protocol	Policy Plan for the Students and Education Domain: policy and guidelines for the careful processing of personal data (adopted in 2020)