

Institutional affairs

GENERAL PRIVACY POLICY

2023

STATUS Definitive
VERSION: 1.0 – translation for public use
AUTHOR Institutional and Legal Affairs
DATE 20-06-2023

Content

1.	Introduction and purpose.....	3
2.	Applicability	3
3.	Mission and risk appetite	3
4.	The privacy organisation	4
4.1.	Organisation	4
4.1.1.	First line - Line responsibility.....	4
4.1.2.	Second line - Institutional and legal affairs	5
4.1.3.	Third line - Data protection officer	5
4.1.4.	Ultimately responsible - Executive Board	5
4.2.	Privacy regulations, work processes and PCF.....	6
4.2.1.	Visual representation of privacy policy	7
5.	Report and improve.....	8
6.	Annex 1 - division of roles (RACI).....	9
7.	Annex 2 - profile privacy champion	10
8.	Annex 3 - structure of reporting P&C cycle	12
8.1.	Privacy	12
8.1.1.	VU-wide privacy priorities.....	12
8.1.2.	Concrete improvement plans	13

1. INTRODUCTION AND PURPOSE

This document describes how Vrije Universiteit Amsterdam (hereinafter 'VU') handles its legal obligations in the context of personal data protection (hereinafter 'privacy'). It is intended to provide insight into how the VU has organised privacy and the processes to be followed in doing so. As far as possible, the policy seeks to tie in with existing VU organisational and work processes.

This document is not intended to inform data subjects about data processing at VU. This is done in the various regulations (see chapter 4.2). More information can also be found on the VU website: [Privacy Statement Vrije Universiteit Amsterdam - More about - Vrije Universiteit Amsterdam \(vu.nl\)](#)

This document is a translation. In the event of any ambiguity or uncertainty arising from the translation, the original Dutch version shall take precedence and govern the interpretation and understanding of the content.

2. APPLICABILITY

This policy is a data protection policy within the meaning of Article 24 of the General Data Protection Regulation (hereinafter 'GDPR'). This policy applies to all parts of the VU.

3. MISSION AND RISK APPETITE

The privacy policy is in line with VU's mission and core values to take responsibility for people and planet in a responsible, open and transparent manner through scientific and values-driven education, research and valorisation.

Our privacy mission is therefore to ensure that the personal data of students, research participants, staff and other data subjects are processed carefully, transparently and in accordance with laws and regulations.

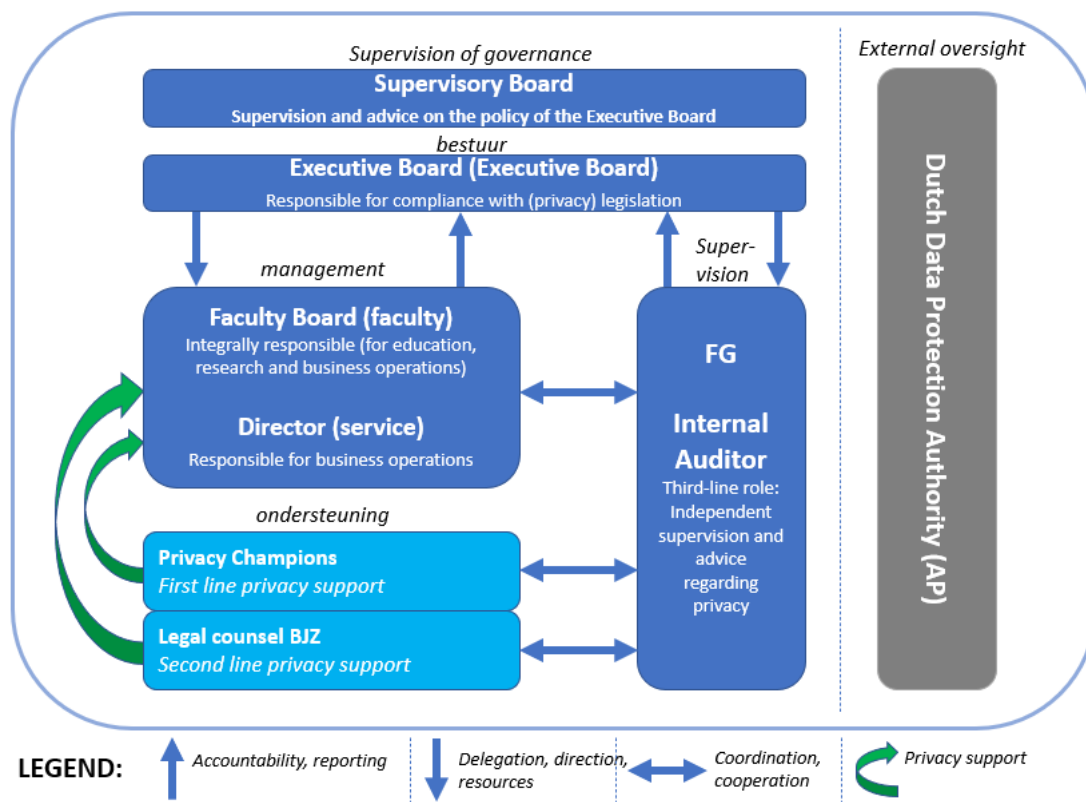
The risk appetite regarding privacy is low. This is in line with VU's risk appetite on other compliance issues. A low risk appetite does not mean that breaches of laws and regulations are excluded, but it does mean that privacy is an established and well-secured part of VU's teaching, research and business operations.

4. THE PRIVACY ORGANISATION

This chapter describes how VU has set up its privacy organisation. As much as possible, alignment is sought with existing structures and VU's governance model.

4.1. ORGANISATION

VU's privacy organisation is set up in accordance with the 'three lines model'¹. The image below summarises this. **Annex 1** provides a further interpretation of the various responsibilities and tasks. Available time, (personal) expertise and, above all, collegiality are factors that partly determine who does what at what time.



4.1.1. FIRST LINE - LINE RESPONSIBILITY

In line with VU's governance model², responsibilities are placed as low as possible in the organisation. This means that each faculty and department is responsible for its own compliance with laws and regulations and privacy policy. This also means that employees themselves bear responsibility. For example, a department head is responsible for his department, a team leader for his team and a researcher is responsible for his research.

Within the faculty board, the director of operations is the portfolio holder for privacy. Within a department, the director is (ultimately) responsible for privacy.

¹ Three Lines Model Updated - July 2020 - The Institute of Internal Auditors.

² VU governance model - 30 June 2015: [Description of VU's governance model](#).

4.1.1.1. Manager

Every manager is tasked with:

- > ensuring that his/her employees are and remain aware of the aspects of the privacy policy and legislation relevant to them; and
- > monitor compliance with the privacy policy within its processes, systems and/or department.

4.1.1.2. Privacy Champions

Every faculty and department has at least one Privacy Champion. The Privacy Champion is the first point of contact for employees with privacy-related questions. The Privacy Champion has a first-line support and signalling role. For complex privacy issues, the Privacy Champion hooks up with BJZ's Privacy Team for second-line support. The full profile of a Privacy Champion is in [Annex 2](#).

Each faculty and department has appointed one or more Privacy Champion(s). To have a functioning and approachable first line, units are encouraged to free up more capacity for Privacy Champions.

When a unit appoints a Privacy Champion, it notifies Institutional and Legal Affairs.

4.1.2. SECOND LINE - INSTITUTIONAL AND LEGAL AFFAIRS

The Institutional and Legal Affairs Department (**BJZ**) makes high-quality legal expertise accessible, no matter how complex the issue. BJZ is responsible for providing legal advice on privacy, maintaining and improving the network of Privacy Champions, having the necessary systems available and providing privacy training. In doing so, BJZ actively contributes to the VU's privacy compliance and helps first-line organisations fulfil their responsibilities.

BJZ coordinates with adjoining disciplines (such as information security, research data management, document management and knowledge security) to ensure that VU's privacy policy remains consistent with the other disciplines.

See also annex 1 for a breakdown of BJZ's activities.

4.1.3. THIRD LINE - DATA PROTECTION OFFICER

The GDPR requires the VU to appoint a data protection officer (hereinafter '**DPO**'). The DPO oversees VU's application of and compliance with privacy legislation. The DPO's legal duties and powers give this officer an independent position in the organisation.

The DPO is a point of contact and enquiry for data subjects who have questions about the protection of personal data. In addition, the DPO coordinates the data breach process and advises on data protection impact assessments (DPIAs). The DPO is the first point of contact for the Personal Data Authority (AP).

Finally, VU's internal auditor, as an independent functionary alongside the DPO, performs VU-wide third-line supervision. The internal auditor monitors the effectiveness of privacy governance, risk management and internal control measures. The internal auditor provides solicited and unsolicited advice to management, the Executive Board and/or the Supervisory Board.

See also Annex 1 for a breakdown of third-line activities.

4.1.4. ULTIMATELY RESPONSIBLE - EXECUTIVE BOARD

The Executive Board (CvB) is ultimately responsible for compliance with laws and regulations. The CvB establishes the policies, measures and procedures around personal data processing with this privacy policy.

4.2. Privacy regulations, work processes and PCF

In addition to this policy, VU has several documents regulating the issue of privacy. Three types of documents can be distinguished:

1. Privacy regulations and privacy statements

These provide VU-wide frameworks and serve as a means of being transparent about what processing of personal data the VU does. For specific processing operations, VU drafts specific privacy statements. An example is the website privacy statement on VU.nl.

With regard to scientific research and valorisation, the VU does not have general regulations. This is because the processing operations in those areas are so diverse that data subjects are informed via specific privacy statements.

2. Work processes

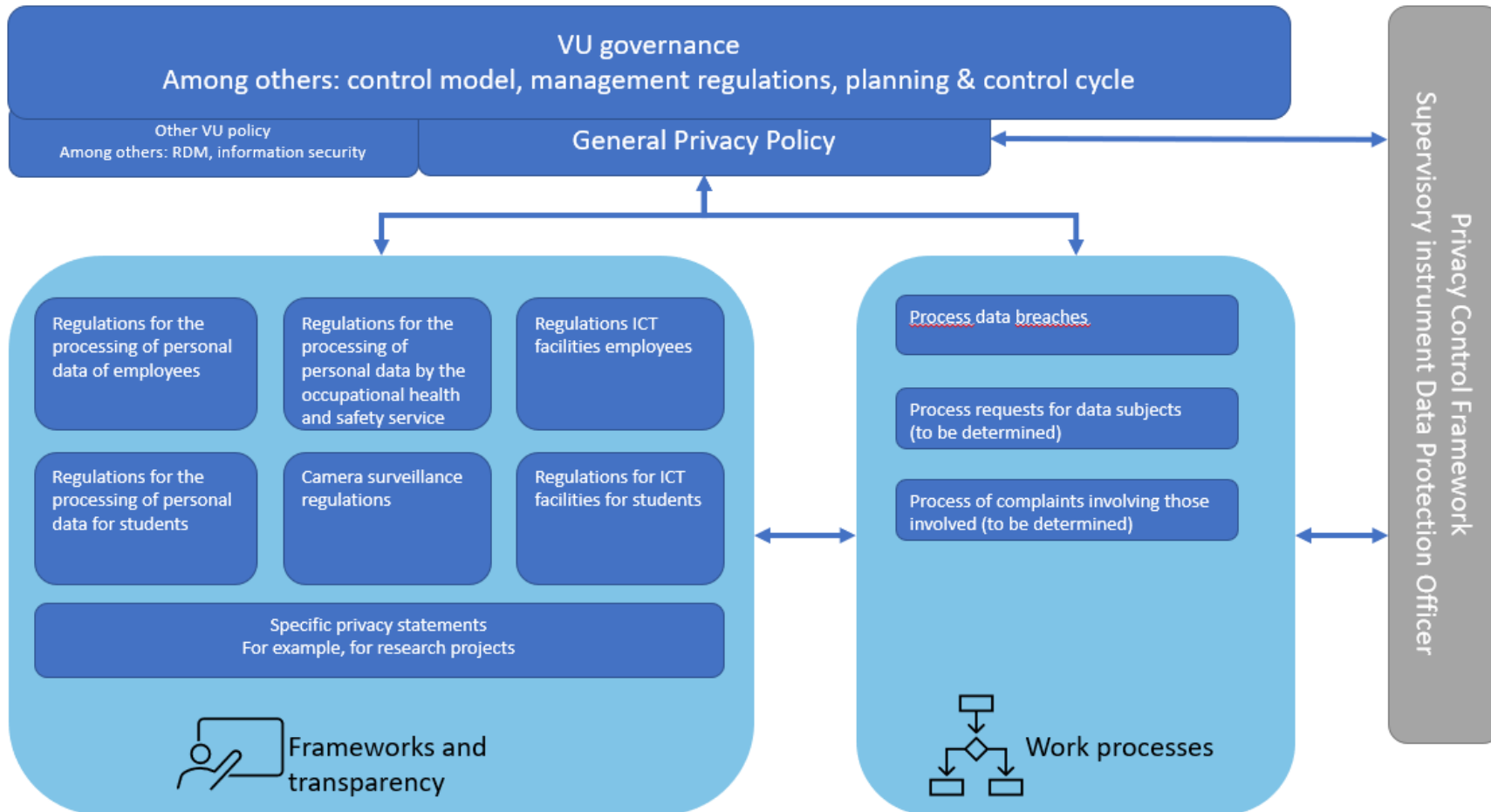
Certain processes related to privacy are set out in documents. These are, for example:

- a. Data breach process ;
- b. Process requests stakeholders; and
- c. Process privacy complaints.

3. Privacy Control Framework (PCF)

The PCF is a risk management system for privacy compliance within VU, which provides insight into how VU has demonstrably designed internal control for privacy compliance. VU's PCF is part of VU's Business Control Framework. The PCF is managed and maintained by the DPO.

4.2.1. VISUAL REPRESENTATION OF PRIVACY POLICY



5. REPORT AND IMPROVE

To make the aforementioned goals and responsibilities work, privacy has been included in VU's planning & control cycle. In concrete terms, this means that faculties and departments include the topic of privacy in their annual plans and report on progress. As a result, the Executive Board maintains insight and overview and has a basis for keeping the Supervisory Board informed.

Annex 3 sets out the reporting format. This set-up is based as much as possible on the current structure of the planning & control cycle.

6. ANNEX 1 - DIVISION OF ROLES (RACI)

Non public annex.

7. ANNEX 2 - PROFILE PRIVACY CHAMPION

Introduction

Privacy and data protection are important topics for the VU. From May 2018, the General Data Protection Regulation (GDPR) will apply. The GDPR brings with it new issues and obligations. To cope with them, knowledge and joint efforts are needed. Faculties and services are responsible for ensuring that their data processing complies with legal requirements. BJZ's privacy team provides support in this, but this cannot be done without the help of so-called "Privacy Champions" who act as the first point of contact at a faculty or department for all privacy-related questions.

Who are Privacy Champions?

The Privacy Champion is the first point of contact at the faculty or department for employees who have questions about privacy. The Privacy Champion makes an active and enthusiastic contribution to raising awareness on the subject of privacy within a (part of a) faculty or department. The Privacy Champion does not need to know *everything* about privacy. He/she does not need to be a lawyer or information security officer, but must have an affinity with the subject and be willing to continue to develop in this area.

The Privacy Champion is visible and accessible. He/she (proactively) brings the topic of privacy to the attention of his/her colleagues and provides first-line support. The Privacy Champion answers the most common privacy questions, such as: May we process this personal data without the consent of the data subjects? Does the VU have a processing agreement with the supplier of this application? May the VU transfer personal data to this organisation?

The Privacy Champion recognises complex privacy issues and knows how to find their way to BJZ's Privacy Team. The Privacy Champion also assists in identifying data breaches and dealing with them. In addition, the Privacy Champion provides support in carrying out Data Protection Impact Assessments (DPIAs).

Finally, the Privacy Champions are the eyes and ears of BJZ's privacy team. The Privacy Champions know what is going on in their department and what is needed in practice. They have short lines of communication with BJZ's privacy team.

To ensure that Privacy Champions have the right knowledge and are and stay abreast of the latest developments, they are trained by BJZ's privacy team according to the 'train the trainer' principle. Optional additional external training should be funded by the units themselves.

Attached is the Privacy Champion profile.

Privacy Champion' profile

Work

The Privacy Champion makes an active and enthusiastic contribution to raising awareness on the subject of privacy within the faculty or department. The Privacy Champion is the first point of contact for the faculty or department in the area of privacy. In addition, the Privacy Champion provides support in completing VU's Register of Processing Activities and carrying out Data Protection Impact Assessments (DPIAs). Furthermore, Privacy Champion is the first contact person within a faculty or department for BJZ's privacy team. The contact person's duties will include the following:

- Contributing to awareness around privacy within the faculty or department;
- answering simple privacy-related questions within the faculty or department (first-line support);
- Providing support in conducting Data Protection Impact Assessments (DPIAs);
- passing on more complex issues to the privacy team and/or other departments and, where necessary, taking a coordinating role in this;
- Identifying privacy risks within the faculty or department and, where necessary, feeding these back to BJZ's privacy team;
- identifying (potential) data breaches and providing support in dealing with them; and
- Contributing to the improvement of privacy-related information provision within the faculty or department.

Training, knowledge and experience

- HBO/academic working and thinking level;
- Knowledge and experience of the (business) processes within the faculty or department;
- knowledge and experience of (research) projects and fulfilling a coordinating role;
- knowledge of personal data protection (privacy) or willingness to acquire it; and
- Knowledge of information security or willingness to acquire it.

Competences

- Good communication skills, both oral and written;
- ability to work well with different disciplines at different levels; - alert, enterprising and environmentally aware; and
- be willing to continue developing in this area.




8. ANNEX 3 - STRUCTURE OF REPORTING P&C CYCLE

To be included in the P&C cycle. Reporting will take place during the P4, P8 and P12.

8.1. PRIVACY




In this chapter, the unit indicates where it stands in terms of privacy policy compliance and how it will improve its privacy compliance in the coming year. Please contact [Institutional and Legal Affairs](#) (BJZ) if you have any questions about this chapter. If in doubt about the most effective actions for the next year, you can always contact BJZ and/or the [Data Protection Officer](#).

Keep in mind that information security is subject to reporting requirements from the [strategic information security policy](#).

	Priorities / targets achieved or on track
	Priorities / targets partly achieved, partly not achieved or on track
	Priorities / targets not met or not on track

8.1.1. VU-WIDE PRIVACY PRIORITIES


In the tables below, indicate which actions your unit will implement. Briefly explain why these actions have been chosen and what goal has been set, or what result the unit is satisfied with.

Priorities VU-wide			
Subject	Describe what the situation in your unit is right now	Describe what goal has been set and what actions you will implement in the coming year to get there	Progress priorities (Do not complete this column until the 12-month report, column do leave it in the annual plan. If possible, please quantify)
Accuracy and completeness of processing register (PrivacyPerfect and DMPonline)			   + explanation
Privacy awareness			
Occupation privacy champions			
Understanding and controlling collaborations and suppliers. How is your overview regarding sharing personal data with external parties. For example, in research consortia.			

8.1.2. CONCRETE IMPROVEMENT PLANS

In this section, answer the following questions:

- For the next year, what are your top three priorities (in addition to those in the previous section), what challenges do you have in doing so and what do you need to achieve them?
- Can activities also be terminated? Which are they and why are they terminated?

Priorities 202X			
A. Concrete improvement actions	B. Priorities and objectives for 2023	C. Priorities ready per:	D. Progress priorities <i>(Do not complete this column until the 12-month report, column do leave it in the annual plan)</i>
Priority 1: ...			 + explanation
Priority 2: ...			
Priority 3: ...			