UNIVERSITEIT VAN AMSTERDAM

Internal Privacy Statement for employees

1. Introduction

This is the Privacy Statement for the use of personal data of employees of the University of Amsterdam (hereinafter: UvA), located at Spui 21, 1012 WX in Amsterdam.
This Privacy Statement describes who we are, how and for what purpose we use your personal data, how you can exercise your privacy rights and any other information relevant to you.

We have tried to provide you with all the information in a way that is clear and easy to read. If you have any questions about our use of your personal data after reading this Privacy Statement, you can contact us using the contact details at the bottom of the Privacy Statement.

This Privacy Statement may change over time. The most recent version of this Privacy Statement can be found on Privacy - University of Amsterdam.

2. To what does this Privacy Statement apply?

This Privacy Statement concerns the personal data of current as well as former employees. The Privacy Statement applies accordingly to other categories of persons performing any work for the UvA. This category includes trainees, guest employees, PhD candidates without an employment contract, temporary employees or contractors, as well as current and former members of the Supervisory Board of the UvA (hereinafter all referred to as employees for convenience). These are just examples. The list is not exhaustive.

3. Who is responsible for your personal data?

The UvA is the data controller for the use of your personal data.

How do we get your data?

In most cases, we get the data directly from you. We may use personal data about you that have been provided to us by a third party. This could, for example, be a recruitment partner, such as a selection office or an employment agency. For employees at a distance from the labour market, for example, we also receive data from the Employee Insurance Agency (UWV), municipal authorities and job coaching organisations, for example.

4. For what purposes do we process your personal data?

The UvA uses employees' personal data for various purposes. These purposes are listed below. Depending on the category of persons, specific purposes 4.1 to 4.9 may or may not apply.

4.1. For entering into an agreement, personnel and salary administration

Entering into an agreement includes: entering into, terminating and performing an employment agreement, guest agreement (guest account), contract for services or internship agreement (hereinafter: agreement); this enumeration is not exhaustive.

When you start working at the UvA, we will use your personal data for the purpose of entering into an agreement with you. We will use your personal data for, among other things, concluding, performing and terminating your agreement.

2025-133860

In addition, your personal data will be used for personnel and (salary) administration purposes. This also covers, for example, the processing of your work assessments, leave and other absence data, travel data, expense data and our communications with you. We will also need to process your personal data due to legal obligations. For example, we will need to do this in the context of mandatory employee identification, fraud prevention, information disclosure to tax authorities, internal control and business protection.

If you have an employment agreement as an employee, we will process your personal data for salary administration purposes. We do this to manage our records related to the payment of your salary, but also to document your hours worked and overtime, as well as any other remunerations and compensations.

If you are a PhD candidate on a 'top-up' scholarship, we will use your personal data for payment of the scholarship.

We will then store these personal data in our personnel administration system and, if applicable, in our student information system and/or promotion registration system. As an employee with an employment agreement, you have access to your (digital) personal data, hours worked, salary slips, invoices and other payment details, annual bonuses, etc.

In connection with the abovementioned agreements and personnel and salary administration, we use various personal data from you. Below is an overview of the personal data we may use for this purpose and the legal basis we rely on in doing so.

Note that, depending on your situation, more or less personal data will be used.

Agreement, personnel and salary administration (absence file) (Part 1/2)	
Legal basis	Personal data
Performance of the agreement, such as an employment agreement, internship agreement, contract for services, guest agreement or promotion agreement	• Name • Address • Town/city • Contact details (email address and phone number) • Date of birth • Place of birth • Gender • Leave registration • Marital status
	• Partner’s name • Partner’s contact details
	• Employment agreement • Signature • Title • Position and redeployments • Data relating to your working conditions

	• Data relating to your terms of employment • Data regarding staff appraisal and career counselling • Personnel file contents • Personnel number
	• Work experience (previous positions, nature and date of termination) • Degree programmes, courses and internships, including diplomas, certificates and degree certificates (obtained before and during the agreement with the UvA)
	• Scope of employment, including changes therein • Details of current secondary activities • End of employment • Certificate of conduct (VOG) (where applicable) • Other data whose processing is required or necessary for the purpose of the agreement. • Chamber of Commerce and VAT data

(Part 2/2)	
Legal basis	Personal data
Performance of the agreement, such as an employment agreement, internship agreement, contract for services or guest agreement. Complying with a legal duty	Absenteeism registration Financial data, such as IBAN numbers (salaries – including annual statements, wage tax statements and payroll taxes – employment conditions and supplementary agreements, reimbursements, expense claims, tax and premiums) Attachment of earnings data Personnel file contents Maternity/parental leave Data concerning illness (registration/correspondence from occupational physician/Employee Insurance Agency (UWV)) Work permit for persons from outside the European Economic Area. Combined work and residence permit.
Complying with a legal duty	Nationality Copy of proof of identity including Citizen Service Number ('BSN')

We will store your data for as long as you are employed by us or there is a valid agreement. Even after you have left employment, we are in some cases obliged to keep your data for purposes for

which there is a legal basis. A comprehensive overview of retention periods for personal data in your personnel and salary administration file can be found in the 'Electronic Personnel File Regulations'.

Types of personal data and where and for how long we keep them.	
The personnel file	Up to a maximum of two years after leaving employment.
The salary administration	Seven years from the financial year (tax retention obligation).
• Name and address particulars • Date of birth • Citizen service number (BSN) • Scan of your proof of identity • Other data for income tax purposes	Up to a maximum of five years after you leave employment (based on the Implementing Regulations to the Wage and Salaries Tax Act).

4.2 Internal elections of members of representative advisory bodies

Legal basis: performance of the employment agreement.

We also store your data for the purpose of allowing you to participate in the elections of representative advisory bodies such as the works council. We use a democratic model for filling positions within these bodies, in accordance with the Works Councils Act. We need data from you so you can stand for election and to invite you to participate in the elections. We use your contact details for this, such as your name, work phone number and work email address.

Your contact details are part of your personnel file and are kept for up to two years after leaving employment.

4.3 To provide you with appropriate development opportunities

Legal basis: performance of the employment agreement.

We use the information from our personnel administration system to offer you appropriate opportunities for the benefit of your career, performance, employability and vitality. This way, we can offer you the right training, education, coaching or other forms of support for your career or personal development. We also use your personal data for general career and talent development.

For this purpose, we process your basic personal data and development-related information such as degree programmes, courses, work and job details, and annual appraisal reports.

We keep your personal data for as long as necessary for your development opportunities. After this period, we will delete your personal data from our systems.

4.4 Protecting your vital interests

Legal basis: vital interest.

If it is necessary to process your personal data in order to safeguard your vital interests, we will do so. We will do this, for example, in the event that you have a medical or other condition that your colleagues or supervisor need to know about, or to get in touch with your specified emergency contacts. Think of an accident or acute illness during working hours. You have provided the medical data to us voluntarily and/or with your consent.

For this purpose, we process your name, contact details, relevant information from your personnel file, insurance details, location and organisations, and the relevant health data you have provided to us.

We will keep your personal data until you leave employment.

4.5 To support your daily tasks and duties

Legal basis: agreement.

When you work at the UvA, you use our systems and networks for your daily work, for example for the purpose of performing education-related activities such as the digital learning environment. You will send emails, search the web, have phone calls, etc.

For this purpose, we use your personal data for the performance of the agreement we have with you as far as metadata are concerned, to allow you to perform your work. We process the metadata of your internet and phone usage, for example, to track and explain the cost of using the equipment provided and to continue to provide appropriate facilities.

We also process IT/workplace/location-related data (account data such as access card number, devices and tools you receive from us (on loan or otherwise), token, IP address, account data (from the ICT systems), content and traffic data (such as your internet communication, received and sent email messages, printed documents and hard copy) and data on backups).

We keep your metadata and account information for 12 months after you leave employment.

4.6 For organisational analysis and development, management reports

Legal basis: legitimate interest.
We use personal data for our business operations to obtain management information and to prepare management reports. We also use your data to implement responsible, effective and efficient HR policies. These statistical analyses focus on examining the impact of the implemented HR strategy. While the management reports and the results of the surveys and related opinions do not contain data that can be traced back to individuals, the source data do contain these data.

The analyses and reports are kept for 10 years after the document is adopted. After this period, we will remove the management reports and the results of the investigations and associated advice.

Your data may also be used for, for example, internal audits, labour and other inspections and company controls.
For handling disputes, we use, among other things, your name, contact details, work and position data, location/organisation and other data necessary for the procedures. We keep these data as long as the dispute is not settled or for as long as is necessary to represent our interests.

4.7 To protect safety and ensure work handover

Legal basis: legitimate interest and consent

We value the protection, safety and integrity of our employees and our office space.

We use camera surveillance. The purpose of this is to protect our company property, protect the property of our employees and visitors, secure access to company premises and parking facilities and record incidents. Camera surveillance takes place at the entrance to and inside our buildings, among other places. The cameras are visibly and invisibly suspended and made known through the use of signs. Camera footage is not used to monitor whether and how work is carried out. Read more about the use of camera surveillance within the UvA in the 'Regulations on camera surveillance'.

The retention period of the camera images is four weeks after the recordings have been made, unless we need the images as evidence in a court case, for example, or after settlement of the observed incidents or after the end of the objection period.

Due to technical management, we may give ourselves access to your mailbox in exceptional situations. This may be necessary, for example, to take care of matters when you have unexpectedly fallen ill or when you are no longer employed by us. We will only do this if you have been informed of this by us in advance and have given your consent. We do not open emails clearly marked as private. We store your personal data for as short a time as possible for this purpose.

4.8 To monitor and investigate compliance with the rules within the UvA

Legal basis: legitimate interest and legal duty.

We monitor our networks, systems and data with the aim of keeping our networks, systems and data secure and uncorrupted. We may do this if you use UvA equipment or use UvA information, networks or systems.

In principle, monitoring takes place at the level of information systems and network traffic, with the logs collected containing only strictly necessary personal data. In the context of network and information security, these logs may be processed to the extent strictly necessary and proportionate to ensure the security, integrity and availability of systems. Targeted monitoring of personal data only takes place when there is a well-founded suspicion that you have broken the rules. In that case, the Executive Board (EB) may order further investigations for a limited, predetermined period. If the rules are violated, the EB may take disciplinary action. The following guidelines and policy rules form the basis for these checks: Responsible use of ICT facilities and policy on the theme of Logging and Monitoring.
To comply with legal regulations, we may also be required to transfer your personal data to government bodies or supervisory authorities.

Among other things, we may use the following personal data to make legal or other decisions and carry out legal or other actions: name, account and profile data (in our ICT systems), the time and date of your logins, the type of information and files you have shared, the searches made with the type of device used, the mobile number of your work device or phone, the IP address of your device, documents you have accessed and the duration of this access, mobile network information, your mobile network provider and which mobile browser you use, your time zone settings and other data that are necessary.

We store the data for up to one year unless you are the subject of internal or external investigation or legal proceedings. In that case, we will store the relevant personal data until the investigation or legal proceedings are completed.

5. Who has access to your personal data?

5.1 Access to your personal data within the UvA

All our employees have access to your profile and the data you have made public on that profile. When you send data to other recipients, such as when you send an email message, that recipient will also receive personal data from you. These data are made accessible on a need-to-know basis within the UvA.

Non-public data can only be accessed by authorised persons in relevant UvA divisions such as IT, CERT, HR, Legal Affairs, the Office of the Rector, and only to the extent necessary to fulfil their respective duties.

5.2 Third-party access to your personal data

The following categories of third parties have access to or obtain your personal data:

Which parties receive your data in any case?		
IT service provider	Dutch Tax and Customs Administration	Employee Insurance Agency (UWV)
Occupational Health and Safety Service	Pension provider	Salary administrator
Insurance companies	Bookkeeper	Accountant
Auditors	Training institutions	Financial, tax or legal advisers
Travel organisations	Banks	Visma Idella
Equivalence	ProActief	
Cooperation partners, such as other educational institutions		

Your personal data will not be shared with other third parties unless required by law.

5.3 The use of your personal data by processors

When a third party processes your personal data on our instructions, that party is a processor. We enter into agreements with processors on the processing of your personal data. In any case, this agreement implies that certain protection obligations will be honoured to ensure that the data are processed in compliance with the wishes and standards of the UvA.

In cases where these processing operations involve the transfer of data to a third party located in a country that does not offer an adequate level of protection, the UvA will take measures to guarantee the adequate protection of the data, such as by entering into standard clauses with the third parties.

6. How are your personal data protected?

The UvA has taken appropriate protective measures to ensure the confidentiality and protection of your personal data. We have implemented appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction of the data, unintentional damage, loss, alteration and unauthorised disclosure or access, and against all other forms of unlawful processing (including, but not limited to, non-essential collection of data) or further processing.

7. How long will your personal data be stored?

We store your personal data for as long as is necessary for the purpose for which they were collected, based on the 'Universities and University Medical Centres Selection List 2020'. Your personal data will be deleted or anonymised when your personal data are no longer necessary for the purposes for which the personal data were processed or when the legal obligations for retention have been fulfilled.

8. How can you exercise your privacy rights?

You have the right to access the personal data we use about you and, under certain conditions, the right to rectification and/or erasure of your personal data. In addition, in certain cases, you also have the right to restrict the processing of your personal data, the right to object to processing and the right to data portability.

To invoke your right to access, rectification, erasure, restriction, object or data portability, contact Legal Affairs at jz-privacy-bb@uva.nl. Please note that Legal Affairs may request additional information to verify your identity when invoking these rights.

If you have consented to the processing of your personal data for a particular purpose, you can withdraw this consent at any time. Please note that withdrawing your consent has no retroactive effect.

9. Lodging a complaint

If you believe that your personal data are being processed in breach of the GDPR, you can submit a complaint to our data protection official (DPO) by sending an email to fg@uva.nl. The DPO is the link between the UvA and the external regulatory authority (the Dutch Data Protection Authority). The DPO acts independently and has a duty of confidentiality.

If you disagree with the outcome of the DPO's handling of your complaint, you can submit a complaint directly to the Dutch Data Protection Authority.

10. When was this Privacy Statement last updated?

30 October 2025