THE AMERICAN UNIVERSITY of PARIS 55 YEARS

PRIVACY POLICY
Faculty & Staff

Policy Number: BP025EN
Issue Date: June 2019

I. About this Policy

The American University of Paris ("AUP", "The University", "we", "our", "us") is committed to protecting the privacy and security of your personal information ("personal data").

This policy describes the ways AUP collects and uses your personal data while you are actively employed at AUP and how we maintain your personal data connected to your employment after you complete your work with us. This policy outlines how we address the responsibilities we hold in relation to the General Data Protection Regulation (GDPR) and related French and United States data protection laws.

It applies to all current and former faculty, staff and interns.

II. This policy's relation to other policies

Separate documents exist detailing how we use personal data related to current students, as well as the use of personal data for student applicants, job applicants, current students, and donors.

Additional personal data use policies will be provided if you use certain services and facilities provided by the University.

Reading this policy and other privacy policies that we may furnish from time to time when we process your personal data is important so that you are familiar with how and why we use your personal data. This policy does not form part of any contract of employment or any other contract to provide services. This policy may be updated at any time.

III. Definitions

'Personal data' means any recorded information that is about you and that allows you to be directly or indirectly identified. Data that has been appropriately anonymized are not included in this definition because your identity has been definitively removed from the dataset.

'Processing' means anything that we do with your personal data, including its collection, its use in decision-making, its storage and maintenance, and its disclosure, deletion or retention.

IV. Who Uses Your Personal Data?

The American University of Paris is considered the "Data Controller" for the personal data processed in relation to this policy (i.e. personal data concerning your time as an employee of AUP). Being the "Data Controller" means that we decide how to use your personal data and are responsible for maintaining and using it in compliance with the GDPR and other data protection legislation.

Access to your employment record and other data covered under this policy is provided to employees who have a need to see as part of their work to fulfill the purposes described in section VI. It is also shared in certain cases with third parties described in section VII.

V. What Personal Data is Processed?

We may process the following personal data, typically obtained directly from you through the application and recruitment process. Some information may be obtained through third parties, such as background check providers, agencies, or reference contacts. We also collect information during your employment with us.

- Personal details (name, address, phone numbers, email addresses, nationality, date of birth, gender, identification documents, etc.);

- Emergency contact information;
- Education and Employment information (schools you have attended and workplaces, courses completed and dates of study, etc.);
- Banking, tax status, and other financial information;
- Salary, leave, pension and benefit information;
- Recruitment information (references, right-to-work, CV, cover letters, etc.);
- Information about your use of our information and communications systems (including CCTV and building access information);
- Disciplinary and grievance information;
- Work-related photographs;
- Information related to your publications, citations, research grants and awards.

We may also process certain information that falls under "special categories" of sensitive personal data.

- Information about your National ID numbers for Immigration (Visa, Passport numbers, Foreigner Number) and tax purposes (Social Security Number);
- Where this is the case, information about your health, particularly any recognized disability
- Trade union membership (for declared union representatives);
- Information about criminal convictions (Only your Bulletin No. 3)

VI. **How the University Uses Your Data**

The University uses your personal data for a variety of purposes, including:

- To assess your suitability to perform a particular role or task;
- To administer salaries, payroll, and pensions, along with other standard functions of employment;
- To administer HR-related processes, including those related to security, discipline, complaints, and audit services;
- To deliver Information Technology services to you and monitor their use;
- To furnish services to you (e.g. library, accommodations, benefits);
- To enable your participation at events (e.g. graduation);
- To communicate with you by email, phone, and mail;
- To support your training and welfare;
- To assess research, including its quantity and impact;
- To compile statistics and conduct surveys and research for internal and external reporting;
- To fulfill our legal obligations concerning immigration and safety;
- To contact you and others in case of an emergency.

The purposes listed above are dependent upon various legal bases including:

1. *When we must meet contractual obligations we have with you*
   Many of the reasons for which we process your data are in order to fulfill the obligations we have to you under our contract with you. Personal data processed based on our contractual obligations includes the data listed in section V.

2. *When we must fulfill a legal obligation*
   Sometimes, your information is processed to meet legal obligations. Information processed for this purpose includes information related to immigration, pension, leave, insurance, and information that we must report to French and US government agencies, such as the *French Academie de Paris*.

3. *When it is necessary to achieve an activity in the public interest*
   In some cases, we process your personal data in the public interest, including documenting conferences, workshops, and invited talks which are open to the public. Research activities and their promotion are also considered to be in the public interest. Generally, teaching and public outreach are tasks that we perform in the public interest so as to fulfill our role as a non-profit corporation and French *association étrangère déclarée en France comme établissement privé d'enseignement supérieur libre* promoting the advancement of learning.

4. *When we need to meet a legitimate interest*

Often, we base our processing of your data on our legitimate interests relating to governance, management, and operation of the University.

For example, we may use your information for:

- Benchmarking
- Internal Communications
- University elections
- Maintenance of IT systems
- Budgets
- Policy Development

5. *When we have your consent*
   There are some situations where we will ask for your consent to collect and process your information. Examples include, but are not limited to, when we ask you to take a survey or when we ask for your permission to collect, process, and share sensitive information.

<u>If you fail to provide the information requested for points 1 and 2 above</u>

Not providing information in certain cases described in points 1 and 2 above means that we may not be able to meet our contractual obligations to you or fulfill our legal obligations. In extreme cases, this may lead to the rupture of your contract of employment.

<u>Purposes of Processing</u>

We process your personal data for the purposes that we collected it for, unless we determine that a reasonable reason exists to use it for another purpose related to and compatible with the original purpose. In the event that we need to use your data for an unrelated purpose, we will seek your consent to use it for the new purpose.

<u>Special Categories of Data</u>

Certain types of data necessitate a higher level of protection. These special categories of data are considered especially sensitive. The University's main operations do not require us to process this type of data regularly but there are some cases where we do. Outside of the cases listed below, we may use these types of data in exceptional circumstances, for example, when it is necessary to protect your or another person's vital interests.

1. *National Identification Number Information (including SSN and Passport/Visa numbers)*
   We will process data concerning your National Identification Numbers only when it is necessary to meet legal obligations. These legal obligations include ensuring that you have met immigration requirements, ensuring that you are provided with appropriate tax documents and that income tax is withheld at the appropriate rate, and ensuring that your income and contributions are properly declared to the authorities in order to provide you with health, retirement and unemployment benefits.

2. *Health Data (Disability Data)*
   We will only process data about your health when it is required to provide accommodations for disability and only as required for legal reporting purposes and for the purposes of occupational medicine.

3. *Criminal Conviction Data*
   We will only process data concerning criminal convictions when it is necessary to meet legal obligations and as it is available on your *bulletin numéro 3*.

4. *Trade Union Membership*
   We will only process data concerning any trade union membership for those employees that are the declared trade union representatives and to meet legal requirements (such as annual negotiations).

VII. Data Sharing with Third Parties and Entities Within and Outside the European Union and European Economic Area

In order to perform our duties based on our contractual and legal obligations or our legitimate interests, we may occasionally share some of your information with parties external to AUP. These third parties may include:

- Relevant Government Agencies (*L'Académie de Paris, Direction Générale des Finances Publiques, URSSAF, Pôle Emploi,* etc.);
- Organizations that help us deliver services to you, including benefits, pensions, etc.
- Internal and External Auditors;
- Employers or prospective employers (where we function as a reference or reference recipient);
- Other educational institutions with whom we may enter into cooperative agreements;
- The media, when we are asked if an employee could offer an expert opinion on a topic;
- External Organizations that provide services to us, such as printing services (name badges, etc.) and the storage and processing of employee data (e.g. ADP).

When information is shared with third parties, we seek to limit the amount of data shared to just what is necessary. Much of the information we share about faculty and staff is reported in aggregated and coded/pseudonymized/anonymized forms.

Any third party that processes data on our behalf must demonstrate that they take measures to protect your data in compliance with the law and with our policies. We never allow them to use your personal data for their own purposes. The University only allows them to process your data for the specific purposes for which we have contracted their services and in accordance with our instructions.

Transfer outside of the European Economic Area - EEA (EU plus Norway, Iceland, and Lichtenstein)
Sometimes, we transfer your data outside the EEA. This may be done when we use a provider that is located outside the EEA, or for other reasons. In all such cases, we ensure that the following conditions are met:

1. Either the country to which the data is transferred is recognized by the EU as providing an adequate level of protection;

   OR

   The organization to which the data is transferred is covered by a scheme recognized by the EU as providing an adequate level of protection;

2. The transfer of personal data is governed by legally-binding contractual clauses between us and the organization receiving the information;

3. The transfer is based on one of the legal bases and is necessary:
   a. To meet the needs of a contract with you or a contract with another person which is in your interests;
   b. To protect the vital interests of you or another person;
   c. To fulfill legal obligations;
   d. To perform functions in the public interest;
   e. To perform functions in our legitimate interest;

   OR

   The transfer has your explicit consent.

Transfers are typically limited situations where the transfer itself is not repeated.

We may display your University email address and telephone number on our websites, which are accessible to internet users, including those in countries outside the EEA.

VIII. Data Security and Retention

Your information and its security is important to us. As such, we have put into place multiple and appropriate measures and safeguards to protect your information.

Your data is kept and retained for the period of your employment at the AUP. After you cease to be an active employee, we archive it for an applicable period or the period necessary for us to meet our legal requirements.

IX. Your Rights and Responsibilities

You have the right to:

- Request access to your data (commonly known as a "subject access request"). This enables you to receive a copy of your data and to check that we are lawfully processing it.
- Request correction of your data. This enables you to ask us to correct any incomplete or inaccurate information we hold about you.
- Request erasure of your data. This enables you to ask us to delete or remove your data under certain circumstances, for example, if you consider that there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your data where you have exercised your right to object to processing (see below).
- Object to processing of your data where we are processing it meet our public interest tasks or legitimate interests.
- Request the restriction of processing of your data. This enables you to ask us to suspend the processing of your data, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your data to another party, subject to the conditions of applicable data portability law.

Depending on your request and its nature, we may not be able to execute what you have asked. For example, when we have a statutory or contractual requirement to process your data and it would be impossible for us to fulfill those legal requirements should we stop processing. For example, for tax purposes we may be required to continue processing your information, even if you object.

When you have given consent for a certain type of processing, you can withdraw the consent at any time. When you withdraw consent, we will stop the processing concerned as soon as possible, however, withdrawing consent does not invalidate prior processing of the information.

Keeping your information up-to-date
It is important that the data we hold about you be accurate and current. Please keep us informed of any changes after you leave the University.

X. Who to Contact and How to Complain

If you want to exercise any of the rights above or you are unsatisfied with how we have processed your information, please contact the AUP Data Protection Oversight Committee at dataprotection@aup.edu. We will treat your request as soon as we can and may keep records of your communications with us to ensure we can resolve your request.

If you remain unsatisfied, you may lodge a complaint with the French *Commission Nationale de l'Informatique et des Libertés* (CNIL).

XI. Changes to this Policy

This policy was last updated 24 June 2019. It is reviewed when necessary and at least once per year. Any changes will be published here and we will inform you of any substantive changes. Occasionally, we may also alert you in other ways about the processing of your data.