

Stanford EU Personnel Privacy Notice

Effective May 25, 2018

We care about our employees and other personnel and know that your privacy is important to you. This Notice is our way of telling you how, in the context of your employment or other working relationship with Stanford, we collect your information, why we need it, and how we use it. This EU Personnel Privacy Notice (“**Notice**”) was published on May 25, 2018. It takes effect May 25, 2018.

Stanford University operates branches (i.e., locations) in Oxford, Paris, Berlin, Florence, and Madrid (together, the “**Stanford EU Branches**”) and each is a **data controller** for the information processed about its employees. As data controllers, the Stanford EU Branches are responsible for deciding how they collect, use and disclose information about their own employees.

The Stanford EU Branches are divisions of Stanford University, which is based in the United States and coordinates activities, including human resource-related activities, across the global organization. The Stanford EU Branches are not separate legal entities from Stanford University. Stanford University is a **joint controller** with respect to your information.

In this Notice, we refer to the Stanford EU Branches and Stanford University collectively as either “**Stanford**” or “**we**”; however, understand that only the Stanford EU Branch where you are located and Stanford University are data controllers with respect to your Personal Information. For example, if you are an employee or other worker located at Stanford’s Oxford Branch, only Stanford’s Oxford Branch and Stanford University are data controllers with respect to your information.

It is important that you read and retain this Notice. This Notice does not form part of any contract of employment or any other contract to provide service.

Scope of Application

This Notice applies to current and former employees, contractors, volunteers, and other workers of Stanford University located in Stanford’s EU Branches (“**EU Workers**”). This Notice also applies to personal data about dependents, family members, next of kin, and beneficiaries of insurance policies and other benefits provided to EU Workers that the EU Worker provided to Stanford University in connection with the EU Worker’s working relationship with Stanford University.

What Information We Collect

During your employment or other working relationship with Stanford, we may collect, store, and use the following information about you:

- contact details (such as name, job title, addresses, telephone numbers, and email addresses);

- date of birth and gender;
- marital status;
- personal data about dependents, family members, next-of-kin and beneficiaries of insurance policies or other benefits provided by Stanford University to EU Workers (including their name and date of birth);
- next of kin and emergency contact information;
- national insurance number;
- payroll information (such as bank account details, payroll records and tax status information);
- benefits information (such as salary, bonus, remuneration, annual leave, pension and benefits information);
- dates and location of employment and information about termination (including related recordings or documents);
- recruitment information (such as copies of right to work documentation, references, background check details, education/qualifications and other information included in a CV or resume);
- employment records (such as work history, working hours, training records, terms of employment or engagement, and performance, grievance, and disciplinary information);
- closed-circuit television (CCTV) footage and other information obtained through electronic means;
- correspondence and information from or about you on and your use of our information and communication systems; and,
- photographs

In addition, we may also collect, store, and use the following **Special Categories** of information about you: information about your nationality, race or ethnicity, religious beliefs, sexual orientation and political opinions; information about criminal convictions and offenses; information about your health (including any medical condition, disability, drug tests, or health and sickness records), and trade union membership.

Beyond the information that you give to us directly (including at the time you applied to work with us and through the recruitment and on-boarding process), we may sometimes collect certain information about you from third parties including the following:

- employment agencies;
- former employers;
- background check providers;
- social media (such as LinkedIn);
- healthcare providers; and,
- benefits providers

We will also collect additional information on an ongoing basis throughout the period of your working with us in the course of job-related activities and in administering our relationship with you.

How We Process Your Information

We will process your information in the following ways:

How we use your information	Why we collect it
Making a decision about your recruitment or employment.	To perform our contract with you and to help us comply with legal obligations to which we are subject.
Checking that you are legally entitled to work in the country where you are employed.	
Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and national insurance/social security contributions.	
Providing you with and otherwise administering benefits.	
Enrolling you in a pension arrangement.	
Administering the contract we have entered into with you.	
Conducting performance reviews, managing performance and determining performance requirements.	
Making decisions about salary reviews and compensation generally.	
Assessing qualifications for a particular job or task, including decisions about promotions.	
Gathering evidence for prospective or ongoing grievance or disciplinary hearings.	
Making decisions about your continued employment or engagement.	
Making arrangements for the termination of our working relationship.	
Fulfilling and tracking education, training and development activities and requirements.	
Managing legal disputes involving you, Stanford or other employees, workers, contractors and third parties, including accidents at work.	
Ascertaining and making decisions as to your fitness to work.	
Maintaining and managing sickness and other absence records.	
Complying with health and safety obligations.	
Monitoring your use of our information and communication systems to ensure compliance with our IT and data security policies.	
Ensuring network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution.	

Satisfying our regulatory obligations.	To help us comply with legal obligations to which we are subject.
Equal opportunities monitoring.	To help us comply with legal obligations to which we are subject and because it is needed in the public interest.
Operating an ethics hotline (including via internal reporting channels) to provide a means by which concerns of unlawful and/or unethical behavior can be reported, investigated and acted upon.	To help us comply with legal obligations to which we are subject and to pursue our legitimate interests to maintain an ethical environment.
Providing information to prospective future purchasers or other business partners, should they arise, in connection with the outsourcing or sale or business combination (including through acquisition) of some or all of the operations or part of the operations in which you work (to explore and capitalize on legitimate business opportunities).	To pursue our legitimate interests in managing our operations as a global organization and to ensure the effective and efficient running of the business.
Running operations, management and planning, including accounting and auditing, marketing and business development, and cost management	
Conducting data analytics studies.	To help us comply with legal obligations to which we are subject and to pursue our legitimate interests to understand our workers' retention and attrition rates.
Providing references and information to future employers.	To help us comply with legal obligations to which we are subject or with your consent.

We typically process Sensitive Categories of information when we need to carry out our legal obligations or exercise rights in connection with your employment or other relationship with us. From time to time, such processing may also be based on a substantial public interest (such as for equal opportunities monitoring). We may also process this type of information where it is needed in relation to legal claims, where it is necessary to protect your interests (or someone else's interests), or where you have already made the information public. In all other cases, we will obtain your consent prior

to processing Special Categories of information. See below, under Your Consent, for further details about obtaining your consent.

Where appropriate, we will collect information about criminal convictions as part of the hiring process or we may be notified of such information directly by you or someone else in the course of you working for us. We will use information about criminal convictions and offences only to confirm suitability for a particular job following an offer of employment or engagement and to process information concerning the alleged commission of an offense in investigating and acting upon concerns reported through internal avenues. We will typically only collect such information where it is appropriate given the nature of the role or where such processing is necessary to carry out our obligations and where we are legally able to do so.

If you fail to provide certain information when requested, we may not be able to perform any contract or agreement we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Your Consent

In certain circumstances, we may ask for your written consent to allow us to process your information in certain ways, including additional processing of Special Categories of information. In any such instances, we will provide you with full details of the information that we would like and the reason we would like it, so that you can carefully consider whether you wish to consent.

In any such circumstances, you have the right to withdraw your consent for that specific processing at any time by contacting Global HR or the University Privacy Office. Upon receipt of any such notification, we will no longer process your personal data for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

When we Share your Information

We may have to share your information with the following third parties:

- Third-party service providers (e.g., payroll processors, third-party benefit administrators, and information technology providers);
- Among affiliated entities within Stanford as part of our regular operations, management, and reporting activities;
- With third parties in the context of a reorganization or restructuring exercise; and,
- With government organizations, law enforcement, regulators, and other third parties when required by law, when it is necessary to administer the employment or other working relationship with you, or when we have another legitimate interest in doing so

We require third parties to respect the security of your information, to process your information only in accordance with our instructions, and to treat it in accordance with the law.

Transfers of Data to the United States

Pursuant to the activities described in this Notice, we may transfer your information to Stanford University, located in the United States. The laws in the United States may not be as protective as the laws in Europe. Because of this, Stanford has taken steps to protect your rights when your information is transferred to the United States through the use of the European Commission's Standard Contractual Clauses. We also take steps to ensure that any onward transfers of your personal data comply with applicable legal requirements.

Storing and Securing your Data

We retain your information for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for your information, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of your information, the purposes for which we process your information and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may pseudonymize your information so that it can no longer be associated with you. We use appropriate safeguards to help secure your information. We will treat your information as confidential and comply with applicable legal data protection requirements when handling your information.

Your Rights

You have the following rights related to the information that we maintain about you:

1. Right of access

You may request details of your Personal Information that we hold. We will confirm whether we are processing your Personal Information and we will disclose supplementary information including the categories of Personal Information, the sources from which it originated, the purpose and legal basis for the processing, the expected retention period, and the safeguards regarding Personal Information transfers to non-EEA countries, subject to the limitations set out in applicable statutes, regulations and other laws.

2. Right of correction

We will comply with your request to edit and update incorrect Personal Information promptly.

3. Right to be forgotten

At your request, we will delete your Personal Information promptly if:

- it is no longer necessary to retain your Personal Information;
- you withdraw the consent which formed the basis of your Personal Information processing;
- you object to the processing of your Personal Information and there are no overriding legitimate grounds for such processing;
- the Personal Information was processed illegally; or
- the Personal Information must be deleted for us to comply with our legal obligations.

We will inform any third parties we might have shared your Personal Information with of your deletion request.

We will decline your request for deletion if processing of your Personal Information is necessary:

- to comply with our legal obligations;
- in pursuit of a legal action;
- to detect and monitor fraud; or
- for the performance of a task in the public interest.

4. Right to restrict processing of your Personal Information

At your request, we will limit the processing of your Personal Information if:

- you dispute the accuracy of your Personal Information;
- your Personal Information was processed unlawfully and you request a limitation on processing, rather than the deletion of your Personal Information;
- we no longer need to process your Personal Information, but you require your Personal Information in connection with a legal claim; or
- you object to the processing pending verification as to whether an overriding legitimate ground for such processing exists.

5. Right to notice related to correction, deletion, and limitation on processing

In so far as it is practicable, we will notify you of any correction, deletion, and/or limitation on processing of your Personal Information.

6. Right to data portability

At your request, we will provide you free of charge with your Personal Information in a structured, commonly used and machine-readable format, if: (i) you provided us with Personal Information; (ii) the processing of your Personal Information is based on your consent or required for the performance of a contract; or (iii) the processing is carried out by automated means.

7. Right to object

Where we process your Personal Information based upon our legitimate interest then you have the right to object to this processing.

8. Right not to be subject to decisions based solely on automated processing

You will not be subject to decisions with a legal or similarly significant effect (including profiling) that are based solely on the automated processing of your Personal Information, unless you have given us your explicit consent or where they are necessary for a contract with us.

9. Right to withdraw consent

You have the right to withdraw any consent you may have previously given us at any time. If you withdraw your consent, this will not affect the lawfulness of our collecting, using and sharing of your Personal Information up to the point in time that you withdraw your consent. Even if you withdraw your consent, we may still use your information that has been fully anonymized and does not personally identify you.

10. Right to complain to a supervisory authority

If you are not satisfied with our response, you have the right to complain to or seek advice from a supervisory authority and/or bring a claim against us in any court of competent jurisdiction.

If you want to exercise your rights, please email us at privacy@stanford.edu]. If you have any questions or concerns, please reach out to Global HR.

Changes to this Notice

We may update this Notice at any time. If we do so, we will make available an updated copy of this notice as soon as reasonably practical. In addition, the current version of this notice from time to time can be accessed on privacy.stanford.edu. We may also notify you in other ways from time to time about the processing of your information.

If you have any questions about this Notice or how we handle your information, please contact [Privacy Office](#) at privacy@stanford.edu.

