

PRINCETON UNIVERSITY – PRIVACY NOTICE FOR [Office of Research and Project Administration]

Princeton University (“Princeton” or the “University”) respects and protects the privacy of your personal data. This notice, which is pursuant to the European Union’s (“EU’s”) General Data Protection Regulation (“GDPR”), contains information about how and why Princeton, through its Office and Research and Project Administration (ORPA), collects your personal data and what we do with that information. The GDPR may apply to the processing of personal information that you provide Princeton while you are in the EU, but it does not apply to information that you provide while you are in the U.S. (for example, on campus).

I. What Constitutes “Personal Data” Under the GDPR?

Personal data is information that Princeton holds about you and which identifies you. This includes information such as your name and institutional address, email and phone number, as well as information like your CV, resume, current funding, or other information an external party requires for processing of grant proposals, awards, and/or subawards.

Under the GDPR, special categories of personal data are afforded an extra level of security and confidentiality. This includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, data concerning health, or data concerning sex life or sexual orientation.

II. How We Collect Personal Data

The personal data that Princeton, through ORPA, holds about you is obtained from a number of sources and may include the following types of information:

- Information provided by you or your collaborators as part of a proposal, award and/or subaward.
- For proposals, names and institutional address/email/phone/fax are stored in the Coeus database rolodex.
- Foreign collaborator’s names and institutions are stored in the Coeus Special Review tab for each proposal, as applicable.
- Proposal attachments, which may include CVs, resumes, and lists of foreign collaborators, are uploaded into the Coeus narrative section and the OnBase database.
- For awards, names and institutional address/email/phone/fax are stored in the PeopleSoft external contacts table.
- Award and subaward documents are uploaded into the PeopleSoft Financials and OnBase databases.
- As part of doing research, contact information is provided to publications.

III. Why We Process Your Personal Data

Our primary reason for collecting and using your personal data is to submit your proposal or process your award and/or subaward in accordance with sponsor and Princeton policies. When you conduct research at Princeton and submit a proposal application through Princeton, and when we accept an award or subaward that supports your research, you should understand that we may

need to process your personal data for administrative purposes. The purposes of processing include, but are not limited to:

- As part of the proposal application, as required by the sponsor;
- In order to process and manage an award or subaward;
- In order to submit subaward payments;
- In order to comply with U.S. government export control regulations, including preparation and submission of export license applications, conduct export control certifications as required by U.S. Immigration and Customs Enforcement for certain categories of visa applicants, review international shipments, review international travel, or to screen foreign collaborators.
- In order to conduct and publish research.
- In order to display information in aggregate in a research dashboard.

IV. Sending Personal Data to Other Countries

For these purposes, personal data may also be transferred to countries outside of the United States or the EU, to countries which may not have data protection laws that offer the same protections as your home country. Examples of circumstances when personal data may be transferred outside the U.S. include:

- Working with PIs, co-PIs, key people, collaborators and/or foreign institutions on proposals, awards, and/or subawards outside the US.
- The sponsor is outside of the US.
- The funding is awarded to Princeton but the research is conducted outside of the US.
- The subaward is to an institution outside of the US.
- The research is being published in a publication outside of the US.

The European Commission has produced a list of countries which, according to the Commission, have adequate data protection rules. The list can be found here:

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

If the country that we are sending your information to is not on the list, or is not a country within the EEA (which means the EU, Liechtenstein, Norway and Iceland), then it might not have the same level of protection for personal data as the EU provides.

Upon request, we will provide you with additional information about the safeguards which Princeton has in place outside of this privacy notice. If you have any questions about the safeguards that are in place, please contact Princeton's Information Security Office at infosec@princeton.edu.

V. How We Share Your Personal Data

We may share your personal data with the following third parties or for the following purposes:

- **With our service providers:** We may share your personal data with third parties that help us provide services to you. For example, ORPA uses software to screen overseas collaborators in order to ensure compliance with export control regulations, and

eShipGlobal for processing of express shipments (FedEx, UPS, DHL).

- **To improve our services:** For example, we may occasionally use consultants, experts, or other advisors to assist Princeton in fulfilling its obligations and to help run the University properly.
- **With government entities:** In response to a valid government request or in accordance with a legal or regulatory obligation, we may share your personal data with a government agency or law enforcement. We may also be required to report certain personal data, for example, to the Department of Education, to comply with our obligations under U.S. law or to protect our rights or the rights of others, or to prevent fraud, waste, abuse, or other criminal activity.
- **With research sponsors:** As part of a proposal application, award and/or subaward agreement.
- **With publications:** As part of the research publication process.

VI. Our Legal Basis for Processing Your Personal Data Under GDPR

This section contains information about the legal bases that ORPA is relying on, for purposes of the GDPR, when processing your personal data.

Legitimate interests

Absent overriding, countervailing interests, Princeton may process your personal data for its legitimate interests. Specifically, Princeton has a legitimate interest in:

- Providing students with an education;
- Enabling you to conduct research;
- Safeguarding and promoting your welfare and the welfare of other employees and students;
- Promoting the objectives and interests of the university;
- Facilitating the efficient operation of the university;
- Ensuring that all relevant legal obligations of the university are complied with, such as US government export control regulations; and
- Ensuring compliance with sponsor requirements for proposals, awards and/or subawards.

In addition, your personal data may be processed for the legitimate interests of others.

If you object to Princeton using your personal data in a particular situation, please contact ORPA Director Elizabeth Adams at 609-258-3090 or ehadams@princeton.edu.

Contractual obligation

Princeton may process your personal data as necessary for the performance of a contract, for example a research award or subaward naming you as an investigator.

Legal obligation

Princeton may process your personal data in order to comply with a legal obligation. For example, we may also have to disclose your information to third parties such as the courts, local authorities, government agencies, or law enforcement where legally obligated to do so.

Vital interests

Princeton may need to process your personal data to protect your vital interests, or someone else's, for example to prevent someone from being seriously harmed or injured.

Public interest

Princeton is acting in the public interest when providing students with an education, or conducting not-for-profit research, and we may process your personal data in connection with that public interest.

VII. Processing Special Categories of Personal Data

Special categories of personal data are treated with extra sensitivity. These special categories include: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, health information, and information about sex life or orientation. Princeton may process special categories of personal data under the following legal bases:

Substantial public interest

The processing is necessary for reasons of substantial public interest.

Scientific or historical research purposes

The processing is necessary for scientific or historical research purposes.

Vital interests

To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal claims

The processing is necessary for the establishment, exercise or defense of legal claims. This allows us to share information with our legal advisors and insurers.

Emergency circumstances and medical purposes

This includes medical treatment and the management of healthcare services.

Consent

We may ask for your consent to use your personal data in certain ways. If we ask for your consent to use your personal data, you can revoke this consent at any time. Any use of your personal data before you withdraw your consent remains valid. Please contact ORPA Director Elizabeth Adams at 609-258-3090 or ehadams@princeton.edu if you would like to revoke any consent given.

VIII. How Long We Retain Your Personal Data

We keep your personal data for as long as we need to in order to comply with the sponsor's record retention policy, which may be longer than Princeton's record retention policy.

We may keep certain personal data indefinitely for historical, research, or statistical purposes.

We will also keep your personal data for as long as necessary to comply with applicable record retention laws and obligations.

For additional information about Princeton's record retention practices, please see Princeton's "University-wide Records Management Principles" (<https://records.princeton.edu/policies-procedures>).

IX. Your Rights Under GDPR With Regards to Your Personal Data

Subject to certain limitations and conditions, you have the following rights with regards to the processing of your personal data:

- **Right of access:** You have the right to request access to the personal data that we hold about you.
- **Right of rectification:** You have the right to correct personal data that we hold about you that is inaccurate or incomplete.
- **Right to erasure:** In certain circumstances, you have the right to request that certain personal data we hold about you be erased from our records.
- **Right to restriction of processing:** In certain circumstances, you have the right to restrict certain processing of your personal data.
- **Right of portability:** You have the right to request that personal data we hold about you be transferred to another organization.
- **Right to object:** You have the right to object to certain types of processing of your personal data, such as direct marketing (to the extent applicable).
- **Right to judicial review:** In the event that we refuse a request under rights of access, we will provide you with a reason. Individuals in the EU have the right to object as outlined in the "Further Information and Guidance" section below.

X. Further Information and Guidance

Please contact ORPA Director Elizabeth Adams at 609-258-3090 or ehadams@princeton.edu should you have any questions or concerns about how ORPA maintains and uses your personal information.

If you believe that we have not acted properly when using your personal information, you can file a complaint with the appropriate supervisory authority in the EU (http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm).

10-9-18