

EEA General Data Protection Regulation Privacy Notice - University of Rochester Applicants and Current Employees Located in the EEA

This Notice describes the practices of the University of Rochester (the “University”) with respect to the collection, use, storage, and disclosure of Personal Data covered by the European Union’s General Data Protection Regulation relating to applicants or employees of the University who are located in the European Union and the European Economic Area (the “EEA”). This Notice applies only to the use of Personal Data in EEA Processing Activities.

In this policy,

- “**GDPR**” means the European Union’s General Data Protection Regulation;
- “**Personal Data**” means information that relates to an individual who is directly or indirectly identified or identifiable; and
- “**EEA Processing Activities**” means the collection, use, processing or sharing of Personal Data when those activities are within the scope of the GDPR.

In this Notice the words “we”, “us” or “our” refer to the University of Rochester, including its Office of Human Resources, and the word “you” or “your” refers to all applicants or employees of the University in the EEA.

Personal Data We Collect

We collect, store, and process a variety of Personal Data in circumstances that may involve EEA Processing Activities. The University collects the following categories of Personal Data relating to applicants or employees of the University:

- Contact information;
- Work history;
- Education history;
- Certifications and licenses;
- Date of birth and social security number;
- Immigration status and work authorization;
- Gender, ethnicity, race, disability status and veteran status;
- Dependent contact and personal information ;
- Immunization and health records;
- Union affiliation (as part of your University employment); and
- Banking information.

How We Collect Personal Data

Personal Data collected includes data that you provide when you complete your application and hire forms and forms you provide during your employment. We also collect data from third

party sources during the application and onboarding processes and throughout your employment with the University. Examples include the following:

- Social media and job board websites that you may have used to apply for a job.
- The background checking agencies used to check your criminal history and educational background.
- Form I-9 systems, employment verification systems and unemployment claims management systems.
- State, Federal and other licensing agencies where professional licensing is verified.
- Systems you and the University use for employment training.
- Systems you and the University use for tax compliance.
- Pre-employment health information through our Occupational Health systems.

Purpose and Legal Basis for Processing Personal Data

Uses and Processing of Personal Data generally includes the following:

- Evaluating your application, resume and documentation provided by you for employment consideration.
- Processing background checks based on forms that you complete to confirm your qualification and work authorization (if a position is offered).
- Administering pre-employment physical assessments after an offer has been made and providing health updates and flu shots (for medical center employees).
- Communicating to you about employment related information or University related activities, notifications or interests.
- Enrolling you (and family members) in University benefits and administering benefits for you.
- Providing systems accesses for your work related duties.
- Administering payroll and providing employment verifications for you.
- Providing your union with required information.
- Responding to inquiries made by you.
- Meeting requirements of government, funding or accrediting agencies.
- Responding to subpoenas, court orders or other legal process to meet our legal obligations.

The University's lawful bases for processing your Personal Data include the following: (i) the University's legitimate interests, (ii) to carry out our responsibilities under a contract, to process transactions requested by you or in order to take steps at your request prior to entering into a transaction or contract, (iii) to comply with laws applicable in the European Union or its member states, or (iv) your consent, where applicable. With respect to item (i) above, the University has a legitimate interest in processing employment applications, hiring and retaining qualified employees, administering employment related functions and complying with laws and regulations that govern our conduct in the countries where we operate.

How We Share Personal Data

Your Personal Data will be received and processed by University representatives in connection with the purposes of processing described above. We may share your Personal Data among University divisions, programs and initiatives. We also share your personal data with third parties who provide transactional and other services on our behalf to administer human resources services and provide systems access including third party training services and background checking agencies. We share your Personal Data with such service providers only when they have agreed to process your Personal Data only to provide services to us and have agreed to protect your Personal Data from unauthorized use, access, or disclosure.

We may also disclose your Personal Data to legal or government regulatory authorities as required by applicable law. We also disclose your Personal Data to third parties as required by applicable law in connection with claims, disputes or litigation, when otherwise required by applicable law, or if we determine its disclosure is necessary to protect the health, safety, rights or property of you, us or others, or to enforce our legal rights or contractual commitments that you have made.

How We Protect Your Data

The University of Rochester uses risk-assessed administrative, technical, and physical security measures to protect against unauthorized use, disclosure, alteration, or destruction of the personally-identifiable information we collect. Only authenticated users with specific permissions may access the data. We encrypt your data in transit using secure TLS cryptographic protocols. We use network segmentation and monitoring to evaluate any attempts at accessing the systems without permission. We maintain a documented vulnerability management program which includes periodic scan, identification, and remediation of security vulnerabilities. Critical patches are applied to servers and workstations on a priority basis. We also conduct regular internal and external penetration tests and remediate according to severity for any results found. All University of Rochester Information Security Policies and Procedures are based upon current industry best practices and common security frameworks.

Your Rights

You have certain rights regarding your Personal Data, subject to certain exclusions as described in the GDPR. This Notice summarizes what these rights under the GDPR involve and how you can exercise these rights. More detail about each right, including exceptions and limitations, can be found in the applicable text of the GDPR.

- Right of Access – You have the right to request that the University confirm whether it is processing your Personal Data. If the University is processing your Personal Data, you have the right to access that Personal Data, and the University will provide you with a copy of that Personal Data unless prevented by applicable law;

- Right of Rectification – You have the right to request that the University correct any inaccurate Personal Data that it maintains about you;
- Right of Erasure – You have the right to request the erasure of Personal Data that the University maintains about you in certain circumstances;
- Right to Restrict Processing – You have the right to request that the University restrict the processing of your Personal Data where one of the reasons identified in the GDPR apply;
- Right to Data Portability – In certain situations, you have the right to request a copy of your Personal Data in electronic format so that you can transmit the data to third parties, or to request that the University directly transfer your Personal Data to one or more third parties;
- Right to Object to Processing – In certain situations, you may have the right to object to processing of your Personal Data;
- Right to File Complaint – You have the right to file a complaint with your applicable European Union supervisory authority if you believe that the University’s processing of your Personal Data violates the GDPR.

In addition, if the basis for processing your Personal Data is consent, you may revoke your consent at any time. Note that, in certain cases, we may continue to process your Personal Data after you have withdrawn consent and requested that we delete your Personal Data, if we have a legal basis to do so.

Data Retention

The GDPR requires that your Personal Data be kept no longer than necessary. The applicable time period will depend on the nature of such personal data and will also be determined by legal requirements imposed under applicable laws and regulations. The University’s current Policy on Retention of University Records is available here: <https://www.rochester.edu/adminfinance/records.html>.

International Data Transfers

Personal Data that you provide while in the EEA will generally be transferred to the United States. If your Personal Data was collected or stored in the EEA, we may transfer your Personal Data outside the EEA and when we do so, we rely on appropriate or suitable safeguards recognized under data protection laws. The European Commission has adopted standard data protection clauses, which provide safeguards for personal information transferred outside of the EEA. We may use Standard Contractual Clauses when transferring Personal Data from a country in the EEA to a country outside the EEA. Where applicable, you can request a copy of our Standard Contractual Clauses by contacting us as set forth in the Contact Information section below. We may transfer your Personal Data from a country in the EEA to a country

outside the EEA after having obtained your explicit and informed consent. We may also transfer your Personal Data outside the EEA if (i) the transfer is necessary to the performance of a contract between you and the University, or if the transfer is necessary to the performance of a contract between the University and a third party, and the contract was entered into in your interest, or (ii) the transfer is necessary in order to protect your vital interests or of other persons, where you are physically or legally incapable of giving consent.

Policy Updates

We may change this Notice from time to time. We will publish on our website any changes we make to this Notice and notify you by other communication channels where appropriate.

Contact Information

If you have any questions, comments, requests or concerns about this Notice, you may contact Kathy Miner, Director of University Human Resources Administration Services, at kathy.miner@rochester.edu or 585-275-7045.