General Data Protection Regulation Compliance
Rose-Hulman Institute of Technology

Overview

Rose-Hulman Institute of Technology (the Institute) is committed to safeguarding the privacy of personal data of students, employees, alumni, contractors, and other constituents, collectively defined "**data subject**", in the General Data Protection Regulation (GDPR). As a "**data controller**", the Institute, collects, uses, and discloses "data subjects" information in accordance with the Institute's *Information Technology Security Policies and Procedures* and in compliance with the EU General Data Protection Regulation.

General Data Protection Regulation

Effective May 25, 2018, the European Union ("**EU**") General Data Protection Regulation ("**GDPR**") places additional obligations on organizations that control or process personally identifiable information about persons in Europe. The GDPR is designed to protect the privacy of personal data concerning a natural person that is collected or processed in or transferred out of the EU, and to regulate the data privacy practices of entities that offer goods or services in the EU.

The GDPR defines (a) "**personal data**" as information that identifies you, or may be used to identify you, such as your name, an identification number, location data, an online identifier, or factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity, (b) **"controller"** as the entity that determines the purposes and means of the processing of personal data, (c) "**processor**" as the entity that processes personal data on behalf of the controller, and (d) **"data subject"** as a natural person who is identified, or can be identified, by reference to his or her personal data.

Legal Bases for Processing Personal Data

The GDPR requires personal data to be processed lawfully, fairly and in a transparent manner, limited only to the data which is necessary, maintained for accuracy, stored only for the length of time required or needed, and safeguarded for unauthorized disclosure. Processing includes performing a task with the personal data such as collection, recording, storage, alteration, retrieval, disclosure by transmission, dissemination, or otherwise making the data available.

When subject to the EU GDPR, the Institute must have a lawful basis to process a data subject's personal data. Although there will be some instances where the processing of personal data will be pursuant to other lawful bases (e.g. processing necessary to protect the vital interests or safety of a data subject, processing related to legal action involving the Institute, etc.), the Institute will likely process personal data relying on one or more of the following lawful bases:

- Processing for the purposes of the legitimate interests pursued by the Institute or by a third party;
- Processing for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing for compliance with a legal obligation to which the Institute is subject; and
- Processing pursuant to the consent of a data subject for one or more specific purposes.

How Rose-Hulman Institute of Technology uses Personal Data

In order for the Institute to achieve its mission, it is necessary to collect, process, and store personally identifiable information for purposes of:

- Recruiting, enrolling, delivering instruction, and awarding academic credit, badging or certificates of completion to students
- Managing residence life, athletic programs, student organizations and other student programming
- Delivering and managing campus health and wellness services
- Recruiting, employing, and compensating faculty and staff
- Fundraising and engagement management
- Conducting Institute business (e.g.. legal, financial, contractual, facility, or programmatic)

Personal Data Sources

The Institute receives personal data from multiple sources, most often directly from the data subject or under the direction of the data subject who has provided it to a third party (e.g., application for admission Common App, College Board, etc.)

Refusal to provide personal data requested in connection with one of the above legal bases for data collection may render it impossible for the Institute to provide education, employment, or other requested services.

Personal Data Categories

To provide services to students and employees, administer its programs, and perform contractual obligations, the Institute may collect, process, and transfer various types of personal data, including but not limited to: name; application information; attendance; academic records; employment records; wealth screening data, date of birth, and contact information, including phone numbers, email addresses, and mailing addresses.

Data Storage and Retention

Personal data will be retained by the Institute in accordance with applicable federal and state laws, regulations, and accreditation guidelines, as well as Institute practices. Personal data will be destroyed in accordance with the Institute *Record Retention and Shredding Schedule*. Requests for erasure will be honored when not in direct conflict with policy, regulation or Institute guidelines. The manner of destruction shall be appropriate to preserve and ensure the confidentiality of information.

Statement on Data Sharing Practices

The Institute may contract with outside service providers including but not limited to Software As A Service (SaaS) vendors. When necessary, the Institute may share personal data with a third party to receive contracted services. Third party access to data is provided only when the purpose for doing so is directly related to Institute business. Data provided to a third party is usable only as described in a *Covered Data and Information Addendum* to a contract defining the service agreement. Before entering in to such a contract with a third party, the Institute reviews vendor data security practices and seeks assurances that vendors comply with relevant industry best practices or governing standards and laws where appropriate.

The Institute may also provide personal information to third parties when required by applicable law, regulation, legal process or governmental request. The Institute may also share information with third parties in aggregated form, after personally identifiable information has been removed, for higher education benchmarking and/or research purposes.

Breach Notification

In the event there is a data breach involving covered data subjects, the Institute will notify the appropriate supervisory authorities within 72 hours, where feasible, after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. In addition, the Institute complies with state and national breach notification laws. Furthermore, the Institute will also notify individual data subjects of a data breach regarding their personally identifiable information (PII).

Data Subject Rights

Subject to limitations established by legal requirements, Institute policies, and regulatory guidelines, data subjects have the following rights:

- To access the personal data we maintain about you;
- To be provided with information about how we process your personal data;
- To correct or modify your personal data;
- To have your personal data deleted;
- To object to or restrict how we process your personal data;
- To request your personal data to be transferred to a third party; and
- To file a complaint.

Questions related to the Institute's compliance with GDPR may be addressed to:

Rose-Hulman Institute of Technology
Institutional Research Planning and Assessment
Myers Building
812-877-8551
Email: Irpa_dept@rose-hulman.edu

Additional EU GDPR policy information may be found at https://www.gdpr.org/

This policy is reviewed annually and will be updated as required.