Introduction

The European Union General Data Protection Regulation (GDPR) regulates the processing of personal data in any format of a living individual residing within the European Union (EU). “Processing” is any activity involving personal data, including holding and storing it.

The University is the data controller for all personal data that it processes, except where it acts as a data processor on behalf of another data controller. The University’s Data Protection Officer is the Director of Information Security.

Scope

The GDPR applies only to the processing of personal data of “natural persons” located in the EU, and is not limited to EU citizens or residents. The GDPR calls these people “data subjects.” For University purposes, data subjects include, but are not limited to:

- Applicants for admission to any of the University’s academic programs or activities, with respect to personal data and Special Category Data pertaining to them, processed by the University while the applicant resides in an EU member state.
- University students studying abroad in a country that is a member state of the European Union, with respect to personal data and Special Category Data pertaining to them, processed by the University while they reside in an EU member state.
Applicants for employment by the University or any of its units or affiliated entities, with respect to personal data and Special Category Data pertaining to them, processed by the University while the applicant resides in an EU member state.

Employees of the University with respect to personal data and Special Category Data pertaining to them, processed by the University while the employee resides in an EU member state.

Individuals who are subjects of human research with respect to personal data and Special Category Data pertaining to them, processed by the University while they reside in an EU member state.

Policy Statement

Data Regulated by the GDPR

University units, employees, and systems must have a valid lawful basis in order to process personal data as described in this policy. Privacy notices must include the lawful basis for processing, as well as the purposes of the processing.

Personal Data

The University may obtain, hold and process the personal data of data subjects, including personal details, family and social circumstances, education and training records, technological identifiers, and information regarding employment, finances, and research.

Special Category Data

The University may obtain, hold and process Special Category Data from EU Residents, which is data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- data concerning a natural person’s sex life or sexual orientation; or
- genetic data or biometric data processed for the purpose of uniquely identifying a natural person.

The University may obtain Special Category Data from the data subject directly, or in some cases from a third party involved in the services provided by a third party.

In those cases where the University processes data subject’s Special Category Data, and where the data subject has not made the information public, the University will seek and must obtain explicit consent of the data subject unless it requires the data for:

- protection of the vital interests of the student or another person;
- exercise or defense of a legal claim;
- substantial public interest;
- purposes of medical or health care;
- the performance of a contract; or
- some other legitimate interest.

Any University processing of Special Category Data will be consistent with this policy and will relate to the University’s provision of services. Where possible, the University will anonymize the Special Category Data used for monitoring and reporting purposes.
Personal Data of current/prospective Students

The University collects the personal data and Special Category Data of GDPR-covered data subjects who are prospective or enrolled students in order to implement and manage all services and processes relating to students, including student recruitment, admission, registration, teaching and learning, examination, graduation, extra-curricular programs and activities, and other services such as accommodation, student support, counseling, healthcare, career guidance and other services. Information facilitating these purposes is collected and processed; without it, the University would likely be unable to provide its services to these individuals or to others. Information is transmitted between and among various University units for operational reasons as is necessary and appropriate for intended purposes.

The University will make a reasonable effort to obtain consent of student data subjects to collect and process such data; however, other lawful basis for collection and/or processing may apply, so that even without consent, such data collection and processing is GDPR-compliant. For example, collection and processing of data of this nature may be necessary for the performance of a contract under which the University provides services to prospective and/or current students.

Some processing activities also may be performed under a legal obligation—

- where necessary to protect the vital interests of the student or another party (for example, disclosures to external parties to ensure safety and well-being);
- where it is necessary for performing a task in the public interest or in the exercise of official authority (for example, disclosing information for the benefit of public health concerns); or
- where it is necessary for legitimate interests pursued by the University or a third party (in such case, the legitimate interests will relate to the efficient, lawful and appropriate delivery of services, and will not operate to the detriment of the interests or rights of individuals).

The University may disclose data subjects’ personal data and Special Category Data to external agencies to which it has obligations. It may also disclose personal data to examining bodies, legal representatives, police or law enforcement agencies, suppliers or service providers, research institutions, sponsoring organizations, or regulatory authorities. The University may disclose information regarding data subjects’ debt owed to the University to collection agencies in order to pursue the debt.

Personal Data of Employees/Applicants

The University collects and processes the personal data and Special Category Data of GDPR-covered data subjects who are job applicants and employees in order to implement and manage all services and processes relating to employees, including recruitment, hiring and/or appointment, training and professional development, testing, certification, programs and activities, and other services such as accommodation, employee support, counseling, health care, career guidance and other services. Information facilitating these purposes is obtained and processed, and without it, the University might not be able to provide its services to these individuals or to others. Information is transmitted between and among various University units for operational reasons as is necessary and appropriate for intended purposes.

The University will make a reasonable effort to obtain consent of employee/applicant data subjects to collect and process such data; however, other lawful bases for collection and/or processing may apply, so that even without consent, such data collection and processing is GDPR-compliant. For example, collection and processing of data of this nature may be necessary for the performance of a contract under which the University provides services to employees.

Some processing activities also may be performed under a legal obligation—
• where necessary to protect the vital interests of the employee or another party (for example, disclosures to external parties to ensure safety and well-being);
• where it is necessary for performing a task in the public interest or in the exercise of official authority (for example, disclosing information for the benefit of public health concerns); or
• where it is necessary for legitimate interests pursued by the University or a third party (in such case, the legitimate interests will relate to the efficient, lawful and appropriate delivery of services, and will not operate to the detriment of the interests or rights of individuals).

The University may disclose personal data and Special Category Data of data subjects who are employees or job applicants to external agencies to which it has obligations. It may also disclose such data subjects’ personal data to examining, licensing or certification bodies, legal representatives, police or law enforcement agencies, suppliers or service providers, research institutions, sponsoring organizations, or regulatory authorities.

Personal Data of Research Subjects

The University holds the personal data and Special Category Data of data subjects who are subjects of human research in order to implement and manage all services and processes relating to research, including research subject enrollment, intervention or interaction with research subjects, publishing of research data, and other services. Information facilitating these purposes is obtained and processed, and without it, the University might not be able to provide its services to these individuals or to others.

The University will make reasonable efforts to process personal data and Special Category Data of data subjects who are subjects of human research with the consent of the data subject(s) whose personal data or Special Category Data is at issue. However, even without such consent, some processing activities also may be performed under a legal obligation—

• where necessary to protect the vital interests of the research subject (for example, disclosures to external parties to ensure safety and well-being);
• where it is necessary for performing a task in the public interest or in the exercise of official authority (for example, disclosing information for the benefit of public health concerns); or
• where it is necessary for legitimate interests pursued by the University or a third party (in such case, the legitimate interests will relate to the efficient, lawful and appropriate delivery of services, and will not operate to the detriment of the interests or rights of individuals).

Moreover, personal data of data subjects who are subjects of human research may be collected and processed by the University as it is necessary for the performance of the contract under which the University receives research funding.

The University may disclose personal data and Special Category Data of data subjects who are research subjects to external agencies to which the University has obligations. It may also disclose such data subjects’ personal data or special category data to examining bodies, legal representatives, police or law enforcement agencies, suppliers or service providers, research institutions, sponsoring organizations, or regulatory authorities.

Rights and Obligations of the Data Subjects

Individual Rights

Data subjects whose personal data or Special Category Data the University processes, have the following rights with respect to this data:

• The right to request access to their personal data held by the University.
• The right to have inaccurate or incomplete personal data rectified.
• The right to erasure of personal data; provided, however, that this may occur only in those very rare circumstances where the University has no legitimate reason to continue to hold/ process that data, including legitimate reasons such as defense of legal claims. The University generally must maintain basic student records and some employment records indefinitely.
• The right to restrict processing of their personal data in certain situations.
• The right to data portability: Data subjects may request in digital form those portions of the University’s personal data regarding them that pertain to their role at the University. For example, students may request data regarding their academic progress in order to provide it to other institutions or potential employers; and employees may request their respective personnel files.
• The right to object to:
  o the University’s processing of their personal data in certain circumstances such as the sending and receipt of direct marketing material; or
  o automated decision-making without human intervention in certain circumstances.
• The right to withdraw consent in those circumstances where the University’s processing of personal data or Special Category Data is based on the consent of the person whose data is at issue. To withdraw consent, the data subject shall contact the unit that obtained the consent or the University’s Data Protection Officer and follow the instructions provided.
• The right to report a concern regarding the University’s processing of the data subjects’ personal data or Special Category Data by contacting the Data Protection Officer with information describing the concern.

Individual Responsibilities

Individuals have responsibilities with respect to personal data collected/processed by the University, as described in the University’s policies on the various types of personal data it processes. Such policies include, but are not limited to: a) Electronic Privacy; b) Employee Records; c) Health Information Privacy and Security (HIPAA); d) Identification (ID) Care (ISUCard); e) Identity Theft Prevention; f) Information Disclosures, ISU; g) Social Security Number Protection. All members of the University community must familiarize themselves with these policies and are responsible for complying with them.

Data Protection Impact Assessment

Where the University undertakes a type of processing that is likely to result in a high risk to the rights and freedoms of data subjects, the University must carry out an impact assessment of that processing, in consultation with any designated DPO. While the supervisory authority is required to create a list of processing operations that require an impact assessment, the GDPR specifies several scenarios in which impact assessments are required. It also provides requirements for the content of such assessments. The university will employ a risk-based approach to data protection.

Data Protection by Design and by Default

All controllers must implement appropriate technical and organizational safeguards to ensure that any processing of personal data complies with the GDPR, including, as appropriate, data protection policies, data minimization, and pseudonymization.

Individuals who fail to comply with the University’s policies may be subject to University discipline and/or other legal recourse, including without limitation, personal liability under the European Union General Data Protection Regulation.

Resources
Links

- Electronic Privacy Policy
- ISU Information and Technology Policies
- IT Security Website