

# GDPR: Compliance with the European Union General Data Protection Regulation

Effective June 14, 2018

Contact: [Information Technology Services](#)

## Contents

### INTRODUCTION

### SCOPE

### POLICY STATEMENT

### Data Regulated by the GDPR

-Personal Data

-Special Category Data

-Personal Data of current/prospective Students

-Personal Data of Employees/Applicants

-Personal Data of Research Subjects

### Rights and Obligations of the Data Subjects

-Individual Rights

-Individual Responsibilities

### Data Protection Impact Assessment

### Data Protection by Design and by Default

### RESOURCES

## 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.

- 38 • Applicants for employment by the University or any of its units or affiliated entities, with respect  
39 to personal data and Special Category Data pertaining to them, processed by the University  
40 while the applicant resides in an EU member state.
- 41 • Employees of the University with respect to personal data and Special Category Data pertaining  
42 to them, processed by the University while the employee resides in an EU member state.
- 43 • Individuals who are subjects of human research with respect to personal data and Special  
44 Category Data pertaining to them, processed by the University while they reside in an EU  
45 member state.

## 46 **Policy Statement**

### 47 **Data Regulated by the GDPR**

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

### 51 **Personal Data**

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

### 55 **Special Category Data**

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

- 58 • racial or ethnic origin;
- 59 • political opinions;
- 60 • religious or philosophical beliefs;
- 61 • trade union membership;
- 62 • physical or mental health;
- 63 • data concerning a natural person's sex life or sexual orientation; or
- 64 • genetic data or biometric data processed for the purpose of uniquely identifying a natural  
65 person.

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

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

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

77 Any University processing of Special Category Data will be consistent with this policy and will relate  
78 to the University's provision of services. Where possible, the University will anonymize the Special  
79 Category Data used for monitoring and reporting purposes.

80 **Personal Data of current/prospective Students**

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

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

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

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

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

109 **Personal Data of Employees/Applicants**

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

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

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

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

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

### 137 **Personal Data of Research Subjects**

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

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

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

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

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

### 163 **Rights and Obligations of the Data Subjects**

#### 164 **Individual Rights**

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

- 167 • The right to request access to their personal data held by the University.

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

## 189 **Individual Responsibilities**

190 Individuals have responsibilities with respect to personal data collected/processed by the University,  
191 as described in the University's policies on the various types of personal data it processes. Such  
192 policies include, but are not limited to: a) Electronic Privacy; b) Employee Records; c) Health  
193 Information Privacy and Security (HIPAA); d) Identification (ID) Care (ISUCard); e) Identity Theft  
194 Prevention; f) Information Disclosures, ISU; g) Social Security

195 Number Protection. All members of the University community must familiarize themselves with these  
196 policies and are responsible for complying with them.

## 197 **Data Protection Impact Assessment**

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

## 204 **Data Protection by Design and by Default**

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

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

## 211 **Resources**

212 **Links**

- 213 • [Electronic Privacy Policy](#)
- 214 • [ISU Information and Technology Policies](#)
- 215 • [IT Security Website](#)

216