**General Data Privacy Regulation (GDPR)**

**Frequently Asked Questions for the UNIVERSITY Community**

**1. What is GDPR?**

A general privacy law that applies to the personal information collected in or from the EU, or that is related to goods or services offered in the EU, or that involves the monitoring of individuals in the EU. The effective date was May 25, 2018. The penalty for violations can range from a warning to up to €20 million or 4% of UNIVERSITY University’s annual revenue.

**2. What areas of UNIVERSITY may be impacted?**

Any department/office/system/function that collects, uses, or stores information in or from the EU or relating to individuals in the EU may be impacted (see chart below).

**3. Generally speaking, what rights does it convey to individuals?**

* Right to full disclosure about personal data practices, including right to be notified about unauthorized access “without undue delay” (and EU authorities must also be notified within 72 hours)
* Right to access stored data, object to its storage, and make corrections (somewhat similar to FERPA)
* Right to be forgotten (e.g., removed from publicly accessible websites, in some cases)
* Right to restriction of processing (particularly as it related to automated decision making/profiling)

**4. How is UNIVERSITY University Responding?**

UNIVERSITY has created a GDPR working group, comprised ……. who are leading the University’s review and implementation efforts. The University will maintain a central online resource for GDPR and will provide stakeholders guidance on implementation and compliance.

We are taking a four tiered approach to GDPR Compliance

* Education
  + Admin Forums (February and May)
  + Brown Bag Lunch and Learn (March)
  + Multiple “All Depts” notices
  + [www.gdpr.UNIVERITY.edu](http://www.gdpr.UNIVERITY.edu) and other information resources
* University resources and notices
  + Update Privacy Statement
  + GDPR Specific Privacy Statement
  + Add link in Univeristy General Announcement
  + Designation of NAME as GDPR Data Projection Officer
  + EU resource page with GDPR specific notices ([gdpr.UNIVERSITY.edu](https://vpit.rice.edu/policies/regulatory-compliance/gpdr))
* Individual/departmental assessment by Working Group
  + Compliance and Information Security will be meeting with any department that has EU data/individuals/business/research/plans
  + Will be reviewing third party contracts and data applications (starting with largest, or those with specific EU focus)
* Monitor and update
  + As new guidance is posted we will update the community and respond accordingly

**5. What is the possible impact to my department/office, and what specific steps should we consider?**

The GDPR working group will help each department/office identify areas of impact and respond appropriately. This chart will help get you started:

|  |  |  |
| --- | --- | --- |
| **Department** | **Where Might UNIVERSITY be Impacted?** | **Possible Solutions (to be discussed)** |
| **Research/**  **Tech Transfer** | Collaborations and agreements with EU professors or universities that involve collecting or sharing personal information  Studies on EU individuals that involve personal information  Human subject research that involves personal information collected in the EU | Additional grant/contract clauses, expanded consent documents, specific consideration in IRB review  Internal process to handle withdrawn consent  Limit receipt of identifiable data  Note that de-identified data is not GDPR, but if it can be re-identified (i.e., there is a key) then it is GDPR |
| **Faculty, Staff and Students in or from EU**  **and**  **Human Resources** | Correspondence containing personal information with individuals in the EU, or faculty/staff/students that will reside in the EU  Exchanging salary or tax information  Conducting background checks on individuals in the EU | Notification, signed consents, specific coverage of GDPR in University policy  Coordination with third party vendors who process data |
| **Admissions,**  **Financial Aid,**  **Registrar,**  **Online Education** | Correspondence containing student personal information, transcripts or financial information being sent from EU students or parents  Program Application monitoring | Notification, signed consents, specific coverage of GDPR in University policy  Coordination with third party vendors who process data  General GDPR notice in the General Announcements |
| **Study Abroad**  **(including exchange programs and students doing**  **research in EU)** | Correspondence containing student personal information regarding individuals who are on programs in the EU  SOS Insurance | Notification, signed consents, specific coverage of GDPR in University policy  Coordination with third party vendors who process data  General GDPR notice in the General Announcements |
| **Title IX/Clery** | Tracking and reporting incidents in the EU (particularly where one party is not a student) | Signed consent where possible. Notification, signed consents, specific coverage of GDPR in University policy  Document approach to potential conflicts up front  General GDPR notice in the General Announcements |
| **Development/**  **Alumni** | Collecting, storing, and sharing personal and financial information in or from the EU, or relating to individuals in the EU | Signed consent where practical, internal process to respond to requests. GDPR in privacy policy  Coordination with third party vendors who process data |
| **Risk Management** | Sharing and receiving personal information, including with International SOS | Signed consent, privacy notices. Coordination with third party vendors who process data |
| **International Students Office** | Discussions with students or parents who are in the EU regarding personal information. Visa information | Notification, signed consents, specific coverage of GDPR in University policy  Coordination with third party vendors who process data  General GDPR notice in the General Announcements |
| **Public Affairs** | Publically available stories or pictures of faculty, staff or students in the EU | Refer individuals to gdpr.UNIVERSITY.edu.  Consent when practical  Internal process to review and respond to take down requests |
| **Information Technology** | Designated individual as POC for GDPR.  Data loss/breach may require notice to individual within 72 hours | Specific scan/procedure for EU individuals following breach  Internal process to review and respond to take down requests |

**6. What should we all be doing to prepare for GDPR?**

Think about how your department/office/function/research intersects with the EU. Is there personal data involved? Do you monitor individuals in any way? Are there financial transactions with individuals in the EU? What is your legal basis for collecting this personal information? What might need to be updated?

What are the ways that someone in the EU could access you? What are the touchpoints? Think about the vendors, services, and internal and external websites that you use to reach into the EU. Review your contracts, and ask vendors and third parties if they are ready for GDPR (or how they plan to be ready soon).

Reach out to the UNIVERSITY GDPR working group, and we’ll help you conduct an assessment and create a plan.

**7. Where can I find out more information?**

UNIVERSITY University EU GDPR Resource Page

[www.gdpr.UNIVERSITY.edu](http://www.gdpr.rice.edu)

EU GDPR Information site:

<https://www.eugdpr.org/>

EDUCAUSE Resources:

<https://library.educause.edu/topics/policy-and-law/eu-general-data-protection-regulation-gdpr>

**8. Who should I contact for more information or with questions?**

ADD NAMES