

GDPR FAQs for KU-Lawrence Faculty and Staff

1. What is the GDPR?

The General Data Protection Regulation¹ is a European legal framework that sets guidelines for collecting and processing personal data of individuals within the European Economic Area (EEA)². The European Union (EU) adopted the GDPR effective May 25, 2018. While the United States has a patchwork of separate, narrower data privacy laws (e.g., HIPAA for health information, FERPA for student information, and state-specific laws), the GDPR is an expansive protection of personal data that applies regardless of the context in which it is collected or the entity collecting it.

2. Why is the GDPR important?

The GDPR clarifies what organization must do to ensure individual's rights regarding personal data and describes what organizations must do to protect those rights. It applies to organizations located or established within the borders of EEA countries, and it also applies to organizations located outside EEA countries if they offer goods or services to, collect data from, or monitor the behavior of individuals within the EEA, regardless of the organization's location. Failure to comply with the GDPR, if and when applicable, puts KU at risk of noncompliance, including monetary fines, potential civil litigation and reputational harm.

3. What does the GDPR protect?

The GDPR protects the personal data of individuals located in the EEA. This includes the personal data of students, faculty, staff, and other members of the

¹ Regulation (EU) 2016/679. For the full text of the GDPR and official EU guidance on it, see https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

² As of June 11, 2018, the following countries are in the EEA: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the UK.

KU community, such as applicants, web site visitors, visiting scholars, alumni and others, who are:

- Permanently residing in the EEA, including students taking classes online;
- Temporarily located in the EEA and accessing KU services, including services related to academic studies, employment or research; or
- Individuals whose data KU collects as part of a research project that is stored or processed by KU, or KU's agents or contractors.

4. What is the purpose of the GDPR?

The purpose of the GDPR is to make sure that any personal data collected within the EEA is collected, stored, and used:

- to the minimum extent necessary;
- for a legitimate, legal purpose;
- in a secure, accurate and controlled way;
- in a way that is transparent to the people from whom it was collected and respectful of their "right to be forgotten."

5. What are some of the key GDPR definitions?

- Personal data: any information that relates to an identified or identifiable *living* individual. This includes any information that organizations or individuals can use to identify a person. Examples include names, addresses, identification numbers, photos, email addresses, social media posts, computer IP addresses, etc.
- Sensitive Personal Data: any special category of personal data that is subject to additional protections. These are personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying the individual data subject, and data concerning health, sex life or sexual orientation.
- Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- Controller: an entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. In the majority of cases where KU is dealing with a third party with access to personal data, KU is acting as the data controller and is obligated to protect the personal data.
- Processor: an entity which processes personal data on behalf of the controller. In situations where KU is dealing with a third party with access to personal data, the third party is likely acting as the data processor and is obligated to protect the personal data. However, KU has the main obligation of protection as the data controller.

6. Does the GDPR apply to an EU citizen living in the US?

The GDPR will only apply to the personal data of an individual located in the EEA. Any personal data collected outside the EEA will not be subject to the GDPR.

7. Does the GDPR apply to a US citizen going to study abroad in the EEA?

Yes, any personal data collected about an individual while that individual is in the EEA will be subject to the GDPR. Any personal data collected outside the EEA will not be subject to the GDPR.

8. Does the GDPR apply to filing systems made up of hard copies of documents (data recorded physically on paper versus digitally)?

Yes, the GDPR applies to personal data in any format, whether paper or digital or electronic.

9. Does the GDPR apply to data that we store and manage through automation?

Yes, personal data processed and stored through automation is within the scope of the GDPR.

10. Do individuals have specific rights under the GDPR?

Individuals have numerous rights under the GDPR, including:

- to request access to, and a copy of, Personal Data;
- to have inaccurate Personal Data corrected;
- to restrict the use or processing of Personal Data;
- to request the erasure of Personal Data, subject to law or legitimate grounds;
- to data portability;
- to object to processing if public interest or legitimate interest is the basis for processing, subject to legitimate grounds or defense of legal claims; and
- the right to withdraw consent to the use of Personal Data.

11. Will KU have a Data Protection Officer (DPO)?

The DPO for the Lawrence Campus is: Tiffany Robinson, Assistant Vice Provost, Office of the University Registrar, tiffany.robinson@ku.edu. Additional contact information is provided in the [Data Protection Privacy Notice](#).

12. When does the GDPR take effect?

The GDPR is already in effect, as of May 25, 2018.

13. When and why does KU have to comply with the GDPR?

If KU is conducting business (which would include education and research activities) within the EEA, in person, over the web or via a third party, then GDPR applies to us. Specifically, anytime KU is collecting or processing personal data that was collected from the EEA, KU is obligated to comply with the GDPR. Even if KU staff never sets foot in the EEA, or the individual is not a citizen of the EEA, GDPR will apply if the personal data originated within the EEA. This means that the GDPR has far-reaching implications for KU faculty and staff, as well as KU operations, such as admissions, athletics, research and international programs.

14. Does KU have a plan for addressing the GDPR?

KU is implementing a GDPR compliance program. KU has a cross-departmental working group that is collaborating to develop and implement GDPR compliance efforts. Some efforts include data inventory, documentation of the legal basis for processing data, obtaining consent where required, faculty and staff awareness, amendment of third-party contracts and continued monitoring of GDPR guidance and enforcement action. KU will monitor how the GDPR is

interpreted, applied and enforce over time and will adjust the compliance program as needed.

15. What are KU's policies regarding GDPR?

For all campuses, KU has posted a data protection privacy notice that informs members of the public of their potential rights under the GDPR. It is available at <http://policy.ku.edu/general-counsel/data-protection-privacy-notice>.

Faculty, staff, and students at the Lawrence Campus are subject to the general privacy policy, which has been updated for the GDPR. It is available at <http://policy.ku.edu/provost/privacy-policy>.

16. What types of projects may involve data that must be processed in compliance with GDPR?

Any project that involves the receipt of personal data from the EEA will trigger GDPR compliance obligations. An exhaustive list is not possible, but feel free to direct specific questions to the DPO and other contacts, as identified in the answer to Question 11.

17. If I have other questions about the GDPR, or its impact on my department or a specific project, who can I contact for more information?

KU-Lawrence faculty and staff may contact Christine Young-Terpening, Assistant General Counsel, at 913-588-7281 or cyoungterpening@kumc.edu, or Tiffany Robinson, DPO, at 785-864-4423 or tiffany.robinson@ku.edu. For the University of Kansas Center for Research (KUCR) or the KU-Lawrence Office of Research, you may contact the IRB Administrator, Office of Research, at irb@ku.edu.