EU General Data Protection Regulation (GDPR)

Overview

- GDPR is a general privacy law that applies to personal data collected in or from the EU related to goods or services offered in the EU or involving the monitoring of individuals in the EU.
- GDPR will require companies and institutions that process the personal data of EU individuals to meet stringent requirements aimed at protecting the privacy of the data that they process.
- Effective date -- May 25, 2018.
- Penalty for violations can range from a warning to up to $25 million or 4% of an organization's annual revenue, whichever is greater.

Application to an institution of higher education located in the US:

GDPR is extra-territorial – can apply to a university department/office that collects, uses, or stores "personal data" in or from the EU, including:

- Data of individuals living in the EU collected for research purposes
- Data of University faculty teaching in the EU
- Data of University students transmitted while studying abroad
- Data of faculty recruited from the EU
- Data of alumni living in the EU collected during fundraising drives
- Internet browsing data/cookies of individuals living in or visiting the EU
- Data of student applying for admission from the EU

What is considered "personal data?"

"Personal data" is any information related to an individual that can be used to directly or indirectly identify the person, such as name, a photo, an email address, bank account, or a computer IP address.

Personal data also includes special categories of sensitive data identified as racial or ethnic origin, political opinions, genetics or biometrics, health, sexual orientation and criminal records, all of which require a higher level of protection.

What is required for an organization to process personal data from the EU?

- Have a lawful basis to process personal data, including:
  - With specific and unambiguous consent from the individual (or guardian for minors);
  - When necessary to perform or enter into a contract with the individual; or
  - For legitimate interests except when such interests are overridden by the interests of the individual
- Maintain a record of data use activities
- Notify EU authorities within 72 hours of data breach
- Implement appropriate technical and organizational safeguards for personal data (left up to the organization to determine)

What rights does GDPR grant to individuals?

- The right to full and transparent information and communication about personal data practices (such as a privacy notice that states the legal basis for processing the data, the retention period, and the individual's right to complain to authorities)
- The right to access and review, object to, and correct stored data (similar to FERPA)
- The right to "be forgotten" (*e.g.* removed from the university's records when there is no compelling reason for continued processing)
- The right to data portability (transmitted to another controller in data-readable format)
- The right to restrict data use (particularly as it related to automated decision-making/profiling)
- The right to breach notification in certain situations

How is UHS Preparing to Comply with GDPR?

UHS has created a GDPR Task Force to spearhead the university's review and implementation efforts.

The Task Force will be conducting a data impact assessment to understand what UH data will be subject to the GDPR. We need your assistance in promptly completing the questionnaire that each department will receive.