Frequently Asked Questions

What is GDPR?

The General Data Protection Regulation (GDPR) is the new European Union (EU) privacy law governing how institutions handle personal data of EU citizens. The regulation goes into effect on May 25, 2018. Fines for failing to comply can be up to €20,000,000 or 4% of an institution's annual revenue.

GDPR outlines several rights of the individual for explicit consent on how personal data can be used, processed, transmitted, as well as how any such data must be protected. As part of compliance, an institution must document the processes it has in place for collecting, using and managing personal data, and maintain records of consent for such data.

What are the GDPR Principles?

As general principles, GDPR says personal data must be:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with the original purpose
- Adequate, relevant and limited to what is necessary in relation to the purposes
- Accurate and kept up to date, rectified without delay
- Kept in a form that permits identification no longer than is necessary
- Processed in a way that ensure appropriate security of the personal data

How is personal data defined?

Personal data means any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- a name
- an identification number
- location data
- online identifier
- or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

When are we allowed to process personal data?

The conditions for processing personal data under GDPR include:

- Consent of the data subject.
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of a data subject or another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

What is required for consent?

There are several requirements to establish consent under GDPR:

- Consent must be freely given, specific, informed and unambiguous.
- Consent requires some form of clear affirmative action. ("Opt-out" or silence does not constitute consent)
- Consent must be demonstrable. A record must be kept of how and when consent was given.
- Individuals have the right to withdraw consent at any time.

What rights does the individual have under GDPR?

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

When does this policy apply?

Whenever personal data is being collected from a person who is physically present in an EU member state.

How does this policy differ from other data security policies, such as HIPAA or FERPA?

The GDPR provides rights to individuals different from data protection laws in the United States and, in most circumstances, provides individuals with greater rights and controls over their own data.

Does this policy apply to EU students and faculty when they're located in the US?

No. This policy only applies to natural persons physically in an EU member state.

Does this policy apply to U.S. students, faculty and staff when they are in the EU?

Yes. Any natural person in an EU member state has the rights afforded by the GDPR while in an EU member state.