General Data Protection Regulation (GDPR)
Regulation 2016/679

What is GDPR?

- Addresses the export of personal data or PD outside of the European Union (EU).
- Provides protection of natural persons' personal data processing and the free movement of their personal data. Data privacy is a fundamental right of all "data subjects" or "identified or identifiable natural person[s]" ***who are in the EU***, even on a temporary basis.
- Adopted in April 2016 but enforceable on May 25, 2016.
- For more specific information on the GDPR, see attached article entitled, "EU Data Protection Regulations" by Gian Franco Borio.

Baseline Rule

Unlawful to transfer EU personal data outside of Europe unless using one of the following mechanisms:

- Standard contractual clauses adopted by European Commission and approved by EU data protection authorities.
- Express consent (which can be revoked) – consent *must be explicit* for data collected *the purposes* data is use for. Consent cannot be withdrawn retroactively.
- Privacy Shield.
- Binding Corporate Rules.
- Procurement.

Individual Rights of the Data Subject in the EU

- Right to be informed about collection and use of PD.
- Right of Access to their data.
- Right of Rectification, corrections.
- Right of Erasure (right to be forgotten).
- Right to restrict processing.
- Right of data portability.
- Right to object to processing.
- Rights in relation to automated decision making and profiling.

Territorial Scope of GDPR (as applied to US colleges/universities)

- US colleges with their own branch campus or study center located in the EU.
- US colleges sending students to or at local counterparts (exchange programs, faculty-led programs, research programs, internships).

- US colleges *receiving* EU students (most likely out of territorial scope, but still be careful on PD collection).
- For specific activities impacted, see attached "GDPR Compliance Chart".

Applies to ALL "processing" of "personal data"

Personal Data/PD – *Any* information relating to an identified or identifiable natural person (e.g., name, identification number, location data, online identifiers such as IP addresses, images).

Processing - any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means (collection, recording, organization, structuring, storage, erasure or destruction, retrieval, etc.)

PD may not be processed unless there is at least one legal basis to do so:

- Consent from the data subject.
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract (e.g., processing for payroll, admissions, study abroad).
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of the data subject or of another natural 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.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular, if the data subject is a child.

Obligations Tied to Whether the Organization is a "controller" or "processor"

Controller - an organization that collects data from EU residents.

Processor - an organization that processes data on behalf of data controller like cloud service providers or the data subject is in the EU. It also applies to organizations based outside the EU if they collect or process PD of individuals located inside the EU.

Data Breaches

- Under the GDPR, the data controller is under a legal obligation to notify the supervisory authority (one or more individuals from each Member State) without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals.
- There is a maximum of 72 hours after becoming aware of the data breach to make the report. Individuals have to be notified if adverse impact is determined. In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach.

- The notice to data subjects is not required if the data controller has implemented appropriate technical and organizational protection measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.

Penalties and Enforcement

- Breach notification increases risk of enforcement.
- If a college cannot demonstrate that it is taking data protection as seriously as others, it may start to lose out on prospective students.
- The GDPR permits fines up to 20 million Euros or 4% of annual global revenues, whichever is *higher*. Many U.S. organizations wonder how an EU member state could levy a fine against them. The GDPR contemplates several ways an EU member state may sanction a noncompliant organization.

  First, if the American organization has established a location in the EU then they can be sanctioned directly.

  Second, some organizations that process a significant amount of EU data must designate a representative located in an EU member state to work with the regulators to ensure compliance and to accept sanctions from the regulators on behalf of the company.

  Finally, the GDPR asserts its authority over "a controller not established in the Union, but in a place where Member State law applies by virtue of public international law." As the GDPR is not in force, it is not clear to what extent an EU member state would leverage an international treaty with the US, or an agreement with the Federal Trade Commission to enforce its regulation on a company located exclusively in the US without a designated representative in the EU, but they clearly are claiming the right to do so.

Data Protection Officers (DPO)

DPOs must be appointed for all public authorities, and where the core activities of the controller or the processor involve "regular and system monitoring of data subjects on a large scale" or where the entity conducts large-scale processing of "special categories of personal data" such as revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, etc.

A university system or group of related campuses or operations could appoint a single DPO as long as they were all subject to a single "controlling" (i.e., parent) organization.