Bond

HIGHER EDUCATION AND CYBERSECURITY INFO MEMO

JANUARY 19, 2018

Is Your Institution in Control of "GDPR" Compliance?

Effective **May 25, 2018**, the European General Data Protection Regulation ("**GDPR**") imposes new obligations on persons or entities that are "controllers" or "processors" of "personal data"[1] about people in the European Union ("**EU**"). Unlike U.S. or even existing European privacy laws, the GDPR (i) can apply to entities that are located *entirely outside* of the EU, and (ii) applies to "personal data" about *anyone in the EU*, regardless of whether they are a citizen or permanent resident of a country in the EU (each country is a "**Member**").[2]

Institutions in violation of the GDPR could face significant fines. Depending on the nature of the violation, an institution in violation of the GDPR could be fined up to €20,000,000 (which amounts to over US $24,000,000) or up to 4 percent of a company's global revenue, whichever is higher. There is some uncertainty with regard to the methodology that will be used to calculate global revenue for U.S. colleges and universities, but it is unlikely that substantive further guidance will be available on the subject before the GDPR becomes effective in May 2018.

Many U.S. colleges and universities will be subject to the GDPR. For example, your institution likely will be considered a "controller" if, among other things, it:

- has an entity or campus located within the EU;
- accepts applications from students located in the EU;
- employs faculty/staff from the EU;
- has students who participate in study abroad programs in the EU;
- has students/faculty/staff that travel within the EU;
- has students/faculty/staff that participate in research that involves certain data from the EU;
- maintains data regarding alumni from the EU; or
- employs certain vendors within the EU (i.e., "processors") or conducts business within the EU.

What are the Major GDPR Requirements?[3]

Among other things, the GDPR requires an institution to:

- appoint a person to oversee protection of personal data;
- provide notice regarding the personal data it collects;
- provide notice of how it uses any personal data collected;
- record the uses and disclosures it makes of personal data;

---

[1] These Terms are defined below.

[2] Each Member will likely adopt its own rules with respect to GDPR compliance; thus U.S. colleges and universities may need the assistance of local counsel in connection each applicable Member. Currently, the U.K. has indicated it intends to follow the GDPR; however, post-Brexit, it is unclear whether the U.K. will implement its own wholly separate set of rules.

[3] Those of you familiar with HIPAA will note the GDPR requirements are very similar.

- obtain specific consent for collection of certain kinds of personal data;
- allow individuals whose personal data was collected to object to such collection or processing, and ultimately honor an individual's "right to be forgotten";
- ensure that all vendors and third parties to which it provides personal data have adequate privacy and security protections; and
- enter into contracts containing specific provisions when transferring personal data outside of the EU (including transferring within the institution).

Key Definitions

- As mentioned above, the GDPR applies to persons or entities that are "controllers" or "processors" of "personal data."
- "Personal data" is defined as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- A "controller" is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the "processing" of personal data.
- A "processor" is a natural or legal person, public authority, agency or other body which is "processing" personal data on behalf of a controller.
- "Processing" means 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.

Conclusion

The GDPR may require U.S. colleges and universities to adopt new privacy and security policies and procedures, and to modify (i) employment procedures, (ii) data collection (including, but not limited to, data collection for admissions) procedures, (iii) admissions procedures, (iv) applications procedures, and (v) study abroad programs.

If you have any questions about this memorandum, please contact Lisa Christensen, or any other member of our Higher Education Practice Group, or Cybersecurity and Data Privacy Practice Group, or the attorney in our firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS