Do I really need to worry about GDPR?

August 8, 2018

A lot has been written about the European Union's new General Data Protection Regulation (GDPR), which became effective May 25, 2018. Colleges and universities are still sorting through whether it applies to them and how it works. While one bulletin can't cover every detail of GDPR's 99 articles, 173 interpretive recitals and dozens of guidance documents, we can address its basic elements to provide context for your compliance efforts.

GDPR differs significantly from U.S. privacy laws

U.S. privacy laws are industry-specific. If your institution is not a "covered entity" under HIPAA, its restrictions don't apply to your activities. Or, if an individual is not your student, their personally identifiable information is not protected from disclosure under FERPA. Through GDPR, the EU takes a very different approach. It establishes the protection of personal data as a fundamental right belonging to all living natural persons. Generally speaking, it applies in any context in which "personal data" is "processed" by a processor or "controller" (the entity that decides what to do with data and how).

GDPR asserts broad extraterritorial jurisdiction

There are three ways that your institution's activities may be impacted by GDPR:

1. GDPR applies to the activities of an "establishment." The EU interprets "establishment" broadly, to include not only permanent facilities owned in the EU but also when activities are carried out through "stable arrangements." This means that it may apply not just to campuses and centers but also to longstanding programs your institution runs through a vendor or partner institution.

2. GDPR applies when an entity offers goods and services to individuals within the EU. Again, this is interpreted broadly to apply when an entity "envisages" providing services to individuals physically in the EU. You do not need to specifically recruit students in the EU to be offering goods and services there; allowing them to apply for admission or to take online classes is enough.
3. GDPR applies when an entity monitors the behavior of individuals in the EU. This refers to tracking individuals online, including profiling or location tracking.

GDPR's scope is based on geography, not citizenship or residency

Some accounts of GDPR say it applies to EU citizens or residents. In fact, GDPR's scope is geographical – it applies to natural persons physically in the EU whether or not they are EU citizens or residents. That means that it applies when students from U.S. institutions are physically in the EU, even temporarily, such as on study abroad programs.

GDPR's definition of "processing" captures a lot of activity – and inactivity

Central to GDPR are its definitions of "processing" and "personal data." Processing is defined as "any operation performed on personal data, including its 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." This definition is noteworthy, because it includes storage. That means that if your institution is storing the personal data of an individual in the EU, you are considered to be "processing" that data, even if you are not actively using it in any way.

The definition of "personal data" is largely what you would expect, although it includes IP addresses and location data that you would not see in a U.S. law. For the record, the definition is, "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, 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."

GDPR only allows personal data to be processed in limited circumstances

GDPR provides only six "lawful bases" upon which personal data may be processed. Of those, only three are likely to apply to a college or university program: when the data subject consents, when it is necessary for performance of a contract and when it is necessary to pursue the "legitimate interests" of the controller when balanced against the rights of the data subject. For any processing of personal data, GDPR requires the controller to specifically document the basis for processing.

GDPR further restricts processing outside the EU and for "special categories" of data

GDPR prohibits the transfer of personal data from the EU to the U.S., except in certain circumstances. Consent and performance of a contract are lawful bases for such transfers, but not the controller's legitimate interests.

In addition, GDPR defines "special categories" of data for which processing is further restricted. Generally speaking, consent is required to process special categories of data. The definition of special categories includes ones you would expect (e.g. race, sexual orientation) and some you might not (e.g. philosophical beliefs, trade union membership). For the record, the definition is: "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 a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

GDPR compliance requires a collaborative approach

Because of the breadth of GDPR requirements, many stakeholders need to be involved in compliance. Informing data subjects of how their data will be processed, obtaining consents and amending contracts is more than IT can do on its own.

We recommend a few steps to get your compliance efforts started. First, determine which of your activities implicate GDPR.

Common activities and programs that involve the processing of personal data from the EU include student admissions, exchange visitor programs, study abroad, online courses, fundraising and alumni outreach and research. Then, for each program or activity, understand the details of how personal data from individuals in the EU is being processed, where it's being processed and by whom. From there, you can strategize what types of notifications, consents or contract provisions you need and how to address the many other details of GDPR.

Authors