CALIFORNIA CCDS AND THE EU'S GENERAL DATA PROTECTION REGULATION - GUIDANCE

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) went into effect. This law establishes expansive protections for the personal data of individuals located in the European Union (EU), regardless of whether the individuals (identified in the GDPR as "data subjects") are citizens of any of the EU's 28 member nations.

U.S.-based colleges are already well-acquainted with the requirements of the Family Educational Rights and Privacy Act (FERPA.) However, GDPR is broader than FERPA both in whose data is protected and the scope of information defined as "personal data."

GDPR defines "personal data" to include "any information relating to an identified or identifiable natural person." GDPR protects the personal data of all individuals located in the EU and it applies to all organizations involved in the "processing" of personal data. "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data." GDPR applies to controllers or processors of personal data outside the EU any time the processing activities are related to offering goods or services to data subjects in the EU.

This law can potentially impact community colleges in a number of ways, including but not limited to:

- Recruiting someone in the EU to serve on the faculty.
- The admissions process for prospective students who are located in the EU.
- Study abroad programs.
- Offering online courses that a person in the EU can take.
- Keeping the records of alumni who are located in the EU.
- Faculty research using data sets drawn from personal data of individuals located in the EU.

Under GDPR, controllers and processors of personal information must have a lawful basis for processing the personal data of data subjects. If an entity cannot rely on one of the specifically enumerated lawful bases in the GDPR, it must have the individual's express consent. In the event of a data breach, notification must be made within 72 hours of discovering the breach. Controllers of personal data must provide certain specified information to data subjects at the time the data is collected, and controllers are obligated to provide a copy to the data subject, correct the data, and erase the data upon request under certain circumstances.

While most analysts believe that the EU will be more focused on the compliance of large international companies like Google and Amazon, colleges have a significant incentive to comply. Many have noted the steep penalties

associated with non-compliance. The maximum for violation of GDPR is the greater of 4% of an entity's global revenue or $20 million euros (approximately, $23,634,000.00.)

Next Steps

Colleges may wish to assess the various ways in which they may obtain personal data from data subjects in the EU. This should be done across departments and functions in order to gain an accurate picture of a college's GDPR compliance risk. A college would also be well-advised to consult its data privacy counsel and/or insurance company providing cyber coverage. One or both of those entities will have guidance and advice regarding updating privacy notices, obtaining GDPR-compliant consents to collect personal data, and ensuring that notice procedures are in place in the event of a personal data breach.

Please contact your Keenan Account Manager for questions regarding this *Briefing*.