FLORIDA GULF COAST UNIVERSITY

ISSUE 9 | VOLUME 1 | November 2018

Internal Audit

INTEGRITY, OBJECTIVITY, CONFIDENTIALITY, COMPETENCY

On May 25, 2018 the European Union's General Data Protection Regulation (GDPR) became effective. The GDPR establishes protections for the privacy and security of "personal data" of individuals located in the EU, known as "data subjects" under the GDPR. It is important to note that data subjects enjoy this protection regardless of whether or not they are a citizen of any EU member state. The GDPR applies to the "processing" of a subjects' personal data, which is broadly defined to include collecting, organizing, structuring, storing, altering, retrieving, using, disclosing, transmitting, erasing or destroying that data.

Areas of concern for U.S. colleges and universities are: how the rules apply to their overseas programs as well as the data they collect on students and employees who are E.U. citizens.
Universities have three different "buckets" of data most likely to be impacted by GDPR. The first bucket, involves students who are foreign nationals coming to university in the United States or attending the university's locations abroad. Any data you collect on those students — from a name to disability status or grades — will be considered personal data.

Another bucket is human resources data. People who work at U.S. universities may be E.U. citizens, or if a university has operations abroad it is likely to have a number of E.U. employees.

The third major bucket involves marketing. Marketing data tends to be collected without a real eye toward privacy. With GDPR, if a student doesn't apply to your university but does some interaction with your website, and does have marketing interaction with you, that data will also be impacted. It won't be as robust or sensitive as the data you have on your actual students, but a potential student is going to provide you some personal data that is going to have to be protected. The GDPR is about making sure you are doing what you need to be doing and then proving you are doing it via documentation and governance.
Universities should consider focusing initial compliance steps on those requirements of the GDPR where the enforcement risk is greatest. Depending on the particular college or university, such non-compliance could include: Lack of a compliant, updated privacy notice; failure to obtain a data subject's valid consent to collect their personal data when required; and failure to notify the relevant supervisory authority within 72 hours in the event of a personal data breach.

The penalties for non-compliance with GDPR can be steep (the greater of 20 million euros or 4 percent of the global revenue). In addition, data subjects may also bring actions for damages or compensation against an entity that violates its obligations.

It is important to recognize that the GDPR is new and many of the data protection issues that US colleges and universities confront with respect to compliance would undoubtedly benefit from further clarification and guidance. Therefore, it is incumbent upon US colleges and universities to continue to monitor developments as the GDPR matures, while expeditiously taking reasonable steps to comply with its requirements.

Excerpts from:
campustechnology.com/articles/2018/05/24/what-gdpr-means for us higher education.
hmbr.com/news-insight/gdprs-impact-on-higher-education.

Challenge Question

This European Union Regulation came into effect on May 25th 2018. Do you know what GDPR stands for?

a. Gross Domestic Product per Region
b. General Data Protection Regulation
c. Graduate Degree Progress Report
d. None of above

Send responses to Viviana Lauke at vlauke@fgcu.edu by **Friday, November 30th.** Correct responses will be entered into a drawing for a **$15 Dunkin Donuts gift card.**

Internal Audit Staff

Bill Foster, MBA, CPA, CIA, CGAP, CFE, CRMA, CCSA
Director, Internal Audit
590-1709
Carol Slade , CPA, CIA
Senior Auditor
590-1117
Jena Valerioti, MBA
Internal Auditor
590-1708
Viviana Lauke
Staff Auditor
745-4439

Resource Links

FGCU Office of General Counsel

Compliance and Ethics Office

EU GDPR.ORG

ICO Guide to GDPR

Regulation Summary EUR-Lex