WHAT IS GDPR AND WHY SHOULD YOU CARE?

Donald Z. Spicer

Co-Editor International Journal of Innovations in Online Education
Assoc. Vice Chancellor and CIO, University System of Maryland;
E-mail: dspicer@usmd.edu

On May 25, 2018 GDPR, the European Union's (EU) General Data Protection Regulation goes into effect. Because it is an EU regulation, many outside of the EU have not paid much attention. This is changing as organizations come to understand the scope and effect of GDPR. First, it is a regulation and not a law, and as such is potentially enforceable outside of the EU without necessary legal agreement by countries not in the EU. Secondly, the data protection to which it refers is that of individuals resident in the EU or citizens of the EU, wherever they are resident. The focus of the regulation is not of enterprises per se, but of how enterprises hold, process, use, and manage personal data. Enterprises that hold such data are held accountable in a number of ways regarding the security, use, and ownership of that data. The intent is to give control over personal information and privacy to individuals. This editor's note is not intended provide an in-depth analysis of GDPR, but suffice it to say that under GDPR individuals have: the right to know how an enterprise intends to use his/her data; be provided a notice of time for data retention; be given the right to access that data and have errors corrected; have the right to be anonymous (i.e., the data may not necessarily be usable to identify the individual); have the right to have personal data erased; have the right to move data to another processor if so desired; and finally, data processors have to build data privacy and security into the design of data utilization processes.

Recent misuses of data and security breaches in the United States, and elsewhere, are an object lesson as to why such regulations may be necessary. Needless to say, such regulations are not currently in place in the United States, and thus many enterprises that hold personal information do not have the people, processes, or technology to meet the expectations of GDPR. This generally includes universities—public, private, and for-profit.

All this said, universities are not the primary target of GDPR, but are still are subject to its expectations. This goes to the question of why you should care as an online educator. While place-based education may not involve EU citizens or residents in a significant manner, online education is very likely to have students and faculty who are either EU citizens or residents. These individuals, under GDPR, will come to expect certain levels of privacy and data security, and this will be independent of the location of the data holder. Thus, institutions will need the ability to assure these individuals, and respond to their

2377-9527/18/$35.00

requests, that the institutions has processes and technology that meet the expectations of GDPR. While countries do not need to have laws that endorse GDPR, many will have agencies that can enforce its regulations. The United States is in discussion with the EU regarding compliance processes.

So, need online educators be concerned? In the long run universities, which already have FERPA and other privacy processes in place, will have to meet the broader expectations of individual privacy and security of a type described by GDPR. Furthermore, recent abuses and lapses by large data holding enterprises may stimulate legislation in the U.S. In the near term, the main risk, especially in online education, will be lawsuits by individuals related to security and privacy breaches. GDPR will both educate them of their rights and provide a legal framework to request redress. Unfortunately, most institutions of higher education are not prepared to respond.

What should you do? As an online faculty member or administrator, the best you can do is to elevate this issue to appropriate officers of the institution. This is an institutional risk involving business processes and technology. Thus, campus Risk Managers, Attorneys, VPs for Administration, and CIOs are the most likely agents to understand and begin to address this issue. While not near-term, the risk is real in the long-term.