Minimizing the Risks of GDPR for U.S. Academic Institutions

Labor & Employment Law Update

By Jacqueline Lentini McCullough on December 10, 2019

After the implementation of the General Data Protection Regulation (GDPR) in May 2018, U.S. academic institutions continue to grapple with compliance issues. Institutions must address areas where there is exposure to risk and train their employees to minimize that exposure.

One area of risk is the flow of data. Who on campus is the gatekeeper handling the data? Most universities will have a Data Protection Officer (DPO) as required by Article 37 of the GDPR. Other campus GDPR actors may include University Counsel, Information Technology Officers, Information Security Officers, Human Resources, Admissions, Financial Aid, Research, International Programs, Online Education and others specific to an institution. Therefore, all of these employees must be well versed in the rules and consequences of GDPR.

A second area of risk is with third party vendors processing data. It may be difficult to ascertain who the responsible party is with more than one entity touching personal data. For example, a foreign national consents to personal data being processed in the U.S. However, some of the data processed by the U.S. institution may be transferred and stored in *another* non-EU country. Vendor negotiations, contracts and agreements are critical in this regard to protect institutional data.

The extraterritorial scope of the GDPR applies to U.S. institutions, especially those that have campuses in the European Union (EU) for study abroad. Additional documentation is required for student travel to the EU depending on where the personal data is stored, and separate acknowledgements are necessary for photos and video recording. A US institution with EU students *within* the EU must also comply with the GDPR.

Yet another area of risk is the GDPR's Article 17, which indicates EU residents have the"right to be forgotten." In other words, they can request erasure of stored personal data "without undue delay," which may be problematic for institutions. Conflicting relevant U.S. federal or state laws prohibit the immediate deletion of such data. For universities, domestic laws take precedence over the GDPR. There is also a growing threat from fraudulent data requestors. Suspicious GDPR data requests often involve a generic template and must be evaluated individually to determine if it's a legitimate inquiry. In the end, making sure your institution has the right structure in place, to respond to data requests, is critical.

Indeed, you may risk a data compromise or data breach (whereby you allow unauthorized access) simply by not having the requisite protocols in place to verify legitimate inquiries.

Deep GDPR fines have been assessed on certain EU companies across a wide range of industries, but little as of the date of this publication in the area of higher education. Case law highlights include: Google (France fined $57 million), British Airways (U.K. $230 million before Brexit), Unicredit Bank S.A. (Romania over $143k), and a Medical Sector Controller (Austria over $60k).

The GDPR and other privacy laws are still evolving. In 2020, California will enact the California Consumer Privacy Act (CCPA), coined “GDPR Lite,” and detailed in a recent article by my colleagues. It will be one of the most sweeping data collection regulations affecting all U.S. based companies acting as private processors.