Cooley

October 22, 2015

Last week Europe's highest court, the Court of Justice of the European Union (CJEU) declared invalid a "Safe Harbor" framework whereby personal data could be easily transferred between many European countries and the US. The US-EU Safe Harbor Principles were developed in consultation with the EU, the European Commission, and the US Department of Commerce to allow for the efficient transfer of personally identifiable data from the EU to the US in a way that complied with the EU Data Protection Directive (Directive 95/46/EC). Entities could opt-in to Safe Harbor by agreeing, among other things, to comply with a set of privacy principles. The opt-in must be recertified annually, but participants had significant flexibility to assess compliance internally or through an independent party. Safe Harbor was the subject of criticism and skepticism since its inception due to concerns regarding its sufficiency to meet EU data privacy standards. For more information, see our previous alert.

Many US schools and universities have relied on the Safe Harbor framework as the basis of the legality for transferring students' personal data from the European Economic Area (EEA, i.e. the Member States of the European Union (EU) plus Iceland, Liechtenstein and Norway) to the US. What should institutions that have relied on Safe Harbor be doing now in light of the CJEU's decision?

What should US educational institutions and their vendors do now?

As a first step institutions (and third parties acting on their behalf) that are recruiting in the EU should review their data processing and storing activities. (What data is being processed and where?) The key determination is whether personally identifiable data is being transferred from the EEA to the US. If the answer is "no," the termination of the Safe Harbor should not be a matter of concern: only entities transferring personally identifiable data from the EEA to the US would potentially be impacted by the CJEU's invalidation of Safe Harbor. If the answer is "yes," then the Safe Harbor decision could have a significant impact on your organization.

Of course, whether personally identifiable data is being transferred may not be altogether clear. US institutions may be receiving student data from a variety of sources, including the students themselves, the students' current schools, and third party lead generators and recruiters, whether acting for the US school or the student. An institution's response to each of these would be a bit different.

Safe Harbor's invalidation does not prohibit institutions or third parties from transferring data from the EEA to the US; however, institutions and vendors need to ensure that they use accepted alternative transfer mechanisms (see below), which may differ, depending on the circumstances, and in particular the source of the data.

Enforcement based on complaints will vary between countries. In most cases, violations could lead to fines (though criminal penalties are possible in some nations) although jurisdictional questions related to entities with no presence in the EU may complicate enforcement in some cases. The greatest risk for schools and companies may often be the reputational damage associated with perceived violations.

Living with the demise of the Safe Harbor

In most cases, the way to avoid the EU restrictions on the transfer of personally identifiable information is to obtain consent. To be valid, consent must be fully informed, specific and freely given. In practice this means that an institution, or any entity acting on its behalf, must provide the affected individuals (or parents of minor students, which generally means students under the age of 16) with notice that the data will be transferred to the US, and that US laws protecting personal data may be less rigorous than that in the EU. Individuals must also be able to withdraw their consent to the transfer of their data at any time. Finally, consent must be clearly signified: it cannot be inferred from a *failure* to respond (in other words, "opt-out" is not an option).

A basic compliance measure would be for schools to review their existing application and information-provision

processes and to add to those materials the appropriate notifications and certifications. Since virtually all students applying to study in the US are required to complete an application form, usually online, as part of this process, students should be asked to affirmatively consent to the transfer of their information to the US, for example by checking a box disclosing the issue as described above and signifying their agreement to the transfer. Similarly, prospective students asking for information should be asked grant the necessary consent as part of the request.

The issue is more complicated where student data is provided by a third party, which could be the applicant's current institution or a lead generation or recruiting entity or agent. In such case the institution will have no direct contact with the student before the personally identifiable data would be sent and, therefore, cannot obtain his or her informed consent. In such circumstances the institution should protect itself by ensuring that its contract with the third party confirms that the third party warrants that it will obtain the needed consent and that the student data provided to it will be transferred to the US in compliance with all applicable local data protection and privacy laws. It may also be prudent to secure indemnification from third parties acting as agents of the institution in the event that the third party violates applicable data protection and privacy laws.

Final thoughts

Following the CJEU's ruling, many of the EU's data protection authorities have stressed the need for a coordinated response by the member European countries. Guidance is anticipated and it is likely that a grace period will be afforded to allow entities that transfer personally identifiable data into the US to comply with data transfer requirements without the benefit of Safe Harbor. While it remains to be seen what guidance will be given, it would be prudent to consider options, such as those discussed above, to avoid a serious information bottleneck affecting students and prospective students residing in the European countries that are a part of the EEA. How organizations decide to move forward will depend on many factors – obtaining express consent may work for some, but may not be practical for others. And the mechanisms by which you obtain consent could vary based on your specific circumstances. Institutions or companies working with US institutions needing tailored advice on possible solutions to suit their needs should contact Matthew Johnson (US) or Ann Bevitt (UK).

Please connect with your Cooley contact to clarify options in light of the ruling and practical alternatives to suit your business needs. Cooley offers multi-disciplinary depth and experience to clients in data protection, privacy by design, data breach management, incident response, breach preparedness, and related litigation, especially in large breaches and those with multi-national issues.

Key Contacts

Ann Bevitt London	abevitt@cooley.com +44 (0) 20 7556 4264