A SPECTER IS HAUNTING EUROPE: THE GENERAL DATA PROTECTION REGULATION

AND IT SHOULD SCARE YOU, TOO...

By Barmak Nassirian

The European Union (EU) formally adopted a sweeping personal privacy and data safeguarding law, the General Data Protection Regulation (GDPR), in April 2016 with an effective date of May 25, 2018. The GDPR replaced the EU's Data Protection Directive of 1995, and represents a significant expansion of personal privacy rights for EU "data subjects," individuals, regardless of citizenship or permanent residence, who are in the EU while engaged in data transactions, and individuals whose data are "controlled" or "processed" by entities established within the EU.

EU regulations are analogous to federal law in the United States, and are legally binding across all 28 member states, whereas EU directives are broad consensus frameworks that must be individually legislated by member states. The politically challenging effort to enact the GDPR was partially motivated by the desire for uniform protections for all EU residents, and was partially necessitated by regulated entities' needs for consistent compliance requirements across EU member states.

ARE U.S. INSTITUTIONS SUBJECT TO THE GDPR?

Many U.S. entities, including most American colleges and universities, paid scant attention to the enactment of the GDPR because they assumed it would only govern transactions within the EU. However, the GDPR's jurisdiction extends to entities with no presence within the EU if they "control" or "process" covered personal information of EU data subjects.

This limited extraterritoriality, while a significant expansion of the law's reach to entities outside the EU, does not attach to EU citizens abroad. A U.S. entity involved in a data transaction with an EU resident in the United States, for example, would not be subject to the GDPR; the same entity engaging in significant and intentional data transactions with EU residents—whether using old fashioned paper forms or collecting data via the Internet—would be.

In terms of its likely effects on non-EU higher education institutions, the GDPR clearly applies to EU-based operations of foreign institutions, including semester-abroad programs, even if they primarily enroll U.S. residents who may only be temporarily attending programs in one of the member states. Presumably, given their physical presence in the EU and their familiarity with local implementations of the Data Protection Directive, affected institutions would have sufficient awareness of EU privacy mandates to already have engaged in changes to their systems and processes to be in compliance with the GDPR.

A significant subset of U.S. institutions newly affected by the GDPR's extraterritorial reach targets distance education programs to individuals who are physically located in one of the member states. Such programs were generally not subject to EU privacy law under the Data Protection Directive if they did not have infrastructure within the EU, but *will* be covered under the black letter of the GDPR, even if they have no physical presence within the EU. However, Article 3 of the GDPR strongly suggests incidental transactions, such as the mere availability of goods or services via a website, are not automatic grounds for subjecting non-EU entities to the GDPR.

It is tempting to believe U.S. institutions that enroll EU residents in the United States are entirely exempt from compliance with the GDPR. This would certainly be true for EU residents who initiate their admission application process from outside the EU, but most EU applicants start the admissions process from their home countries and obtain visas to enter the United States after gaining admission to eligible programs. In theory, active student recruitment campaigns targeting EU residents could subject the data collected from such students, whether through automated or non-automated means, to compliance requirements under the GDPR.

Beyond the enrollment function, U.S. institutions could also be subject to the GDPR in any joint research and scholarly collaborations with individuals within the EU. As a practical matter, all intentional and regular data transactions with one party located physically within the EU would be covered by the GDPR.

A more precise understanding of how the GDPR will be further defined, interpreted and enforced by the EU and its member states' national data protection authorities will take several years to evolve. It seems unlikely that the most expansive interpretation of the regulation's extraterritorial application would be immediately enforced against non-EU entities.

Institutions with significant engagement with the EU, either through a physical presence or distance-delivered services, should take immediate steps to engage in good-faith compliance. Others should pay close attention to the evolution of the law's compliance requirements over the coming years. These requirements, while not conceptually dissimilar to existing U.S. privacy and data safeguarding statutes and regulations, are more rigorous and high stakes.

EU DATA SUBJECTS AND THEIR RIGHTS

Personal information of all natural persons—i.e, people but not legal entities such as corporations or nonprofits—physically within the EU (EU data subjects) are covered by the GDPR. The regulation makes no distinctions based on individuals' permanent places of residence or nationality. The GDPR applies to all such individuals' personal data, defined as any information that can be used to, directly or indirectly, identify a person. These include not only information such as educational, financial, employment-related, and health data, but also photographs, personal phone numbers, and IP addresses. This definition is virtually identical to the one used in U.S. educational privacy law—i.e., "personally identifiable information" as defined in regulations (34 CFR 99.3) issued under the Family Educational Rights and Privacy Act (FERPA). However, FERPA treats directory information as public by default, while giving individuals the right to opt out. GDPR, in contrast, subjects all personally identifiable data to its core requirements and provides additional protections for "sensitive personal data," including racial and ethnic origin, religion, sexual orientation, political views, etc. It also recognizes the improved security of anonymized and encrypted or fragmented (pseudonymous) data, which it subjects to less stringent requirements.

Beyond mere protection of data, the GDPR articulates a range of additional rights for EU data subjects, including the right to transparency (i.e., that data about them is being collected or maintained), the right to access data, the right to rectify errors in data systems, the right to erasure of personal data (the "right to be forgotten"), the right to restrict processing of data, the right to portability of personal data, and protections against profiling or automated (algorithmic) decisions.

CONTROLLERS AND PROCESSORS

A main difference between the GDPR and American privacy laws is the former's consumer-oriented approach, which regulates virtually all data transactions with people in a non-industry-specific manner. Various U.S. privacy laws, in contrast, address privacy and data practices by sector (e.g., FERPA for education, Children's Online Privacy Protection Rule for children, the Privacy Act for federal data, Health Insurance Portability and Accountability Act for health data). With the notable exceptions of certain foreign policy, national security, and law enforcement data practices, the GDPR applies to all commercial and professional transactions of "controllers" and "processors" of data.

Controllers are the principal entities and main counterparties to transactions with individuals. They are the entities that govern the purposes, uses and methods related to the processing of personally identifiable information. Processors are organizations—typically IT firms—that actually carry out the processing activities. The GDPR does not apply to personal or household interactions among individuals, for example on social networks, but it does cover data practices of any commercial or professional platforms that individuals may use.

In most situations, U.S. universities would encounter the GDPR as controllers, i.e., in a functional capacity as the party that needs certain data to engage in certain activities. There are, however, routine scenarios under which U.S. institutions could function as processors, for example when they serve as a platform for communications that include individuals physically located within the EU.

GDPR: A COMPREHENSIVE DATA GOVERNANCE MANDATE

Another unique feature of the GDPR is that it covers all facets of information management, including the collection, retention, deletion, breaches and disclosures of personal data. No single U.S. privacy or data security law currently governs all of these related issues. The expanded definition of processing under the GDPR has important consequences for privacy practices of covered U.S. institutions for which FERPA has been the primary privacy mandate for over four decades.

Because FERPA only addresses post-collection disclosure practices, U.S. institutions have been generally free to define their own data collection and data retention practices. With minor exceptions, FERPA takes no position on what data institutions may collect or how long they may keep them, focusing instead on who within institutions and which third parties outside institutions may gain nonconsensual access to data. GDPR, however, subjects the entire lifecycle of all personal information, including the collection of specific data elements, to its strictures, and generally mandates the data subject's consent as a precondition for processing activities.

CONSENT

GDPR Article 6 asserts personal consent as a fundamental requirement for most processing activities. Most collection, storage, use, matching and disclosure—including subcontracting of processing functions—of personally identifiable information must be based on the data subjects' consent, either directly or indirectly, through a contract to which the data subject is a party. That consent, furthermore, must be freely given and specific to the transaction.

General waivers of privacy, mandatory consent as a condition of providing services not directly requiring the personal information in question, blanket check-the-box agreements, and automatic opt-ins with optional withdrawals do not satisfy the consent requirement. The consent mandate lies at the heart of the GDPR and includes the right of withdrawal—"the right to be forgotten"—in connection with deletion of personal data that are no longer necessary to the purpose for which they were collected. The specificity of the GDPR consent requirement therefore serves the additional purpose of creating a strong incentive for data minimization as a basic privacy principle.

Articles 13 and 14 of the GDPR specify a series of required disclosures to data subjects in cases where data are collected directly from them or would be obtained from other sources. These include the identity and contact information of controllers and agents, the legal basis and purpose of the data collection, the category of recipients of the data being collected, data retention and deletion policies of the controller, and whether any of the data being collected would be maintained in a third country.

SUPERVISORY AUTHORITIES AND FINES

The GDPR requires EU member states to designate qualified supervisory authorities with specified oversight and investigatory and enforcement powers to implement its requirements. These authorities will oversee compliance, provide consultation and prior approvals, and receive and administratively adjudicate complaints against controllers and processors. They can also impose fines of up to 2 percent of a violator's global revenues for some violations, and up to 4 percent of such revenues for more serious ones. These enormous fines have captured the attention of multinationals, which will drive compliance through contractual indemnification requirements with clients and subcontractors.

Just as important as the supervisory authorities' power to impose penalties is the consultative role they are assigned in reviewing mandatory data protection impact assessments that data controllers and processors must regularly perform in connection with high-risk processing activities prior to implementing them. In addition, GDPR Articles 37-39 describe activities and responsibilities that a subset of controllers and processors, including all non-judicial EU public-sector entities, will have to assign to designated internal data protection officers.

BREACH NOTIFICATION

With some exceptions, the GDPR codifies a mandate for controllers and processors to notify their supervisory authorities of any breaches within 72 hours of their discovery and to provide information on the remedial steps they have taken in response. It also requires breach notification to data subjects themselves "without undue delay."

CONCLUSION

The EU took years to adopt the GDPR, and it is safe to assume that it will take years before the GDPR's real impact and practical compliance requirements become fully settled. The core principles that undergird the GDPR are generally similar to the Fair Information Practice principles in the United States, but their specific EU implementation is decidedly different than how they have been adopted in U.S. law. P

Barmak Nassirian is director of federal relations and policy analysis, AASCU.