AASCU American Association of State Colleges and Universities
Delivering America's Promise

The European Union General Data Protection Regulation (GDPR)

Barmak Nassirian, Federal Director
Thursday, February 22, 2018

The European Union has set an effective date of May 25, 2018, for the

General Data Protection Regulation (GDPR)

GDPR Background

In April 2016, the European Union (EU) formally adopted the General Data Protection Regulation (GDPR) with an effective date of May 25, 2018.

The GDPR, which replaced the EU's Data Protection Directive of 1995, represents a significant expansion of personal privacy rights for EU residents.

EU regulations are akin 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 new regulation started as a data protection directive in 2009.
- Negotiations were between the European Commission (the EU executive body) and its two legislative chambers, the Council of the European Union and the European Parliament.
- The effort was motivated by the desire for uniform protections for all EU residents and by the needs of regulated entities for consistent compliance requirements across the EU.

How is GDPR Different than Directive 95/46/EC?

- The GDPR has a more enforceable legal status in comparison to the Data Protection Directive.
- Significantly more detailed mandates on consumer rights, institutional data governance, information technology practices, and oversight.
- Significantly higher administrative fines:
  - €10,000,000 or up to 2% of the total worldwide annual revenues of the preceding financial year, whichever is higher
  - €20,000,000 or up to 4% of the total worldwide annual revenues of the preceding financial year, whichever is higher
- Greater extraterritorial reach: the GDPR's coverage applies to all "controllers" and "processors" of personally identifiable information about EU "data subjects" within the Union, but it also extends to entities with **no physical EU footprint** if they "control" or "process" covered personal information of EU data subjects.

Why Should US Institutions Pay Attention?

- The GDPR clearly applies to EU-based operations of foreign institutions, including semester-abroad programs.
- The GDPR targets distance education programs to EU residents who are physically located in one of the member states.
- (In theory) active student recruitment campaigns targeting EU residents could subject the data collected from such students, whether via automated or non-automated means, to compliance requirements under the GDPR.
- All intentional data interactions with or monitoring of EU data subjects

Controllers and Processors

- Controllers are the principal entities and the 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 they may use.

EU Data Subjects

- All natural persons—i.e., not corporations or organizations—within the European Union, regardless of whether they are citizens or residents of members states or temporary visitors are covered by GDPR.
- Natural persons located in venues where "Members State law applies by virtue of public international law" are also covered (primarily diplomatic missions and deployed servicemembers of EU member states on overseas assignments).

Data Protection

- The GDPR protects personal information of all natural persons physically within the EU.
- The GDPR applies to all such individuals' personal data, defined as any information that can be used to, directly or indirectly, identify a person (virtually identical to how PII is defined in FERPA).
- Includes:
  - Educational
  - Financial
  - Employment-related
  - Health data
  - Photographs
  - Personal phone numbers
  - IP addresses

How GDPR Is Different Than FERPA

- 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" that include racial and ethnic origin, religion, sexual orientation, political views, etc.
- With some exceptions, FERPA does not mandate data collection and retention practices of institutions, nor does it specifically address data safeguarding requirements.
- GDPR is a comprehensive data privacy, data security, and data mobility framework.

Protections Under Processing

- The GDPR covers all facets of information management including:
  - Collection
  - Retention
  - Deletion
  - Breaches
  - Disclosures of personal data
- No single US privacy or data security law currently governs all of the related issues that the GDPR does.
- The expanded definition of processing under the GDPR has important consequences for privacy practices of covered US institutions for which FERPA has been the primary privacy mandate for over four decades.
- GDPR 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.

With Important Exceptions, Individual Consent Governs the Disclosure, Use and Retention of PII Under GDPR

What Qualifies As Consent

- 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.
- Consent must be freely given and specific to the transaction.

What Doesn't Qualify As Consent

- 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.
- Automatic opt-ins with optional withdrawals.

Important Rights of EU Data Subjects Under GDPR

GDPR, Chapter III, Articles 12-22 articulate a detailed list of new rights for EU data subjects. Controllers should specifically review these to make certain that their practices (and their systems) can accommodate them. These rights track and expand on basic Fair Information Practices (FIPs) principles and address:

- Transparency
- Access
- Rectification
- Erasure ("Right to be Forgotten")
- Restriction of Processing
- Portability
- Objection
- Profiling and Automated Decisions

Supervisory Authorities, Fines, and Judicial Remedies

- The GDPR requires EU member states to designate qualified supervisory authorities with specified oversight, investigatory, and enforcement powers to implement its requirements.
- They will oversee:
  - Compliance
  - Provide consultation and prior approvals
  - Receive and administratively adjudicate complaints
- They have the authority to impose administrative fines of up to 4% of a violators global revenues based on severity of noncompliance.

- In addition, individuals or public interest organizations acting on their behalf can seek compensation through legal action against controllers or processors for any harm due to noncompliance.

Breach Notification

- Controllers and processors have to notify their supervisory authorities of any breaches within 72 hours of the discovery.
- They must provide information on the remedial steps they have taken in response to the breach.
- GDPR mandates breach notifications to data subjects themselves "without undue delay". (A limited right under Article 34)

Cross-Boarder Transfers

- The same restrictions that were in the Data Protection Directive will remain in effect in under the GDPR.
- The legal privacy protections in the US generally do not satisfy EU standards.
- Cross-boarder transfers between the EU and the US are now governed by the Privacy Shield framework, pending the negotiation of a new, more robust safe harbor.

Enforcement

- 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 in the form of physical presence or of distance-delivered services, should take immediate steps to engage in good-faith compliance.
- Others should be paying close attention to the evolution of the law's compliance requirements over the coming years.

Who Should Be In The Final Stages of Implementing GDPR?

- US institutions with EU-based operations or significant numbers of EU residents as students.
- US institutions delivering distance education programs to such students within the EU.
- US institutions engaged in educational, cultural, or scientific exchange programs with EU-based individuals (includes study-abroad and faculty/scholar exchanges).
- US institutions involved in financial transactions with EU-based individuals.

In Conclusion

- The EU's GDPR mandate extends to entities outside EU borders if they engage in data transactions with EU "data subjects."
- The extraterritorial reach of the GDPR is likely to affect most US institutions even if they do not have EU-based campuses or locations.
- The GDPR will likely take years before its real impact and practical compliance requirements become fully settled.
- US institutions with EU-based operations and those with significant data interactions with EU data subjects—particularly those delivering distance education programs to such students within the EU or engaged in exchange programs — should be in the final stages of implementing GDPR-compliant practices now.
- GDPR compliance is not a merely technical issue to be delegated to CIOs, it is primarily a data governance framework that should involve the functional units of the university: admissions, records, international programs, research operations, and the business office.

Overview of GDPR

https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained

Authoritative Information on GDPR Available at

https://www.eugdpr.org/eugdpr.org.html

For questions or information about this webinar please contact Emily Parker, parkere@aascu.org or 202.478.4659