



AN OVERVIEW

OF THE

GDPR



On May 25, the European Union's General Data

Protection Regulation (GDPR) goes into effect, standardizing

data protection law across all 28 European Union countries. The overarching goal of the GDPR is to protect EU citizens from privacy and data breaches.

“The GDPR is a legal framework that gives us guidelines for the collection and processing of personal information for individuals in the European Union,” says Melissa B. Musser, Director of Risk Advisory for Aronson LLC, an accounting and financial consulting firm based in Rockville, MD. “Once you get through all the new lingo, which can be overwhelming, it’s basic blocking and tackling. We should already know what data we have and why we think we have the right to process it.”

Some of the most notable effects of the GDPR on universities are related to study abroad programs, international students and faculty with EU ties. Consider just a few scenarios where personal data comes into play: A U.S. student who spends a semester abroad enrolled in a Spanish university. A university staff member who attends a recruitment fair in Denmark and collects data from interested attendees. A collaborative research project conducted by faculty in both the U.S. and the European Union.

“GDPR will apply to universities,” says Musser. “They need to identify what students, faculty and alumni are going into and coming from the EU. They need to document their information and understand where it’s coming from and how they are monitoring particular information.”

THE EU'S GENERAL
DATA PROTECTION
REGULATION HAS
RAMIFICATIONS ON
YOUR UNIVERSITY.



TERRADOTTA



HIGHLIGHTS OF THE GDPR

Interpretation of the GDPR and compliance with it are legal issues. Because the nuances of the regulation are complex, universities should work with a legal team and risk advisors to ascertain how the new regulation specifically affects them. However, it's beneficial to have a high-level understanding of the GDPR.

The GDPR, which replaces the 1995 EU Data Protection Directive, extends the protection of personal data and associated rights. "It's a very thoughtful regulation that says, 'You know what organizations? You don't own this information. The person owns their information,'" says Musser. "The GDPR is working to give rights back to the individual."

Some of the key points of the GDPR include the following:

Expanded notion of personal data

"The definition of personal information has been expanded to include anything that can identify a person directly or indirectly, such as location," says Musser. "If someone can find your address, they're going to know it's you."

Increased territorial scope

The GDPR applies to any organization processing personal data of people residing in the EU no matter where the organization is located.

Condition for consent

The GDPR strengthens the conditions for consent: Consent must be given in a clear, intelligible and easily accessible form. It also must be simple to withdraw consent.

Breach notification

Any breaches of the GDPR must be reported within 72 hours of becoming aware of the breach.

Right to access

People have the right to know whether their personal data is being processed, where and for what reason.

Data erasure

People have the right to request their data no longer be processed and be erased.

Privacy by design

The inclusion of data protection needs to be considered from the outset when designing systems: It can't be an "add-on" feature.

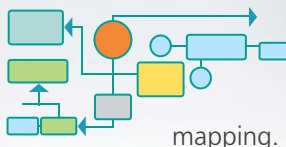
Levels of responsibility

The GDPR specifies two levels of responsibility. The "controller" determines the purposes and means of processing personal data, while the "processor" processes personal data on behalf of the controller.

FIRST STEPS TOWARD COMPLIANCE

“Two years ago, Gallaudet University in Washington, D.C., formed a Data Governance Committee. The committee has several focuses it promotes including the sharing of business knowledge and data, best practices between campus units, and optimization of internal information management.” The committee has begun to consider the GDPR and how to ensure compliance.

“Our tech people bolstered our breach protection after an Educause conference about GDPR last fall, and we do periodically test our general privacy compliance,” says Pamela Rypkema, Risk Manager at Gallaudet University. “We have been identifying and evaluating specific interaction we have with the EU. We hope to adopt more proactive best practices over this calendar year.”



One of the first steps that Musser suggests universities like Gallaudet take is data flow mapping. “A lot of universities already have information security processes in place,” she says. “I think what has not been done yet is a data flow map—a true map of the different categories of people that universities hold data on. This includes employees, alumni and students.”

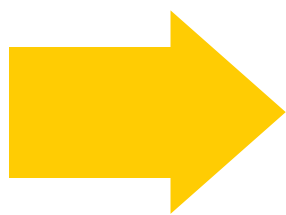
Musser encourages schools to categorize people, then ascertain what data they hold on each group. Next,



consider the business need and lawful basis for processing that information. Once you’ve established a legal basis, then implement the appropriate controls to prevent the data from coming to harm. To do that, you will need to know how the information is flowing from inception to interaction with third parties.

“There are a lot of layers to the GDPR, but once you’ve done the basic data flow mapping then it makes everything else less overwhelming,” says Musser. “You can look at everything in pieces.” She recommends working with the data protection officer or risk management staff at your university. She also advocates looking at what other universities have done to see if you can leverage some policies or forms. For example, the City University of New York has posted a GDPR student consent form online.

FIVE RESOURCES ON THE GDPR



For more in-depth information on the General Data Protection Regulation, try these resources:

The European Commission’s website on data protection

An interassociation guide to the GDPR that specifically examines its implications on higher education

A webinar on the GDPR presented by University Risk Management and Insurance Association Inc. (URMIA)

EUR-Lex provides free access to all European Union laws, including text of the complete GDPR

The United Kingdom’s Information Commissioner’s Office offers numerous resources on data privacy, including ones related to the GDPR

Disclaimer: This article serves as an overview to help universities become familiar with the EU General Data Protection Regulation. It is not intended, nor can it be relied upon, as legal advice.

THE BROADER BENEFITS

The U.S. doesn't currently have a comprehensive framework for data protection, although two bills were recently introduced in the Senate. Instead, there's a hodge-podge of sector-specific federal laws (like HIPAA in healthcare) and state laws (48 states have data breach notification laws). Even so, Musser believes universities should consider implementing policies that adhere to the spirit of an inclusive law like the GDPR. "Even if the GDPR doesn't apply to certain aspects of data collection and processing, we should still use it," she says. "I think this is where things are headed."

Rypkema also sees value in careful, comprehensive data protection—both on a practical level and universally. "A campus can eliminate the cost, effort and risk exposure of collecting worthless data and, instead, focus resources on accurately collecting valuable data and efficiently storing it so to easily retrieve it when an appropriate use comes up, but to block it when hackers and others want to misuse it," she says.

Perhaps more importantly, protecting personal data creates goodwill among stakeholders such as students and alumni. "Protections and controls can set a tone at the top that guides decision-making throughout the organization and demonstrates to people that data is valued, special and protected," says Rypkema. "Over time, hopefully this enhances the institution's reputation and relationship with various stakeholders."



TERRADOTTA

ABOUT TERRA DOTTA

Our mission at Terra Dotta is to offer the very best products and services in higher education software. We are committed to delivering a user-experience that transforms the way our clients operate and engage with their constituents. We accomplish this through the continual deployment of best-in-class technology, and the focus we place on mutual trust in each and every one of our business relationships. These values form the Terra Dotta difference.

For additional information please visit www.terradotta.com