Scenario
Lucia, a citizen of Spain, is a student in Barcelona. She is soon to finish her high school (bachillerato) experience and plans to attend college to study computer science. Her parents are encouraging her to attend university in the United States. Lucia’s father is a proud alum of a US institution of higher education and makes regular donations to his alma mater.

From her bedroom, Lucia goes online to learn more about US colleges and universities. Lucia knows that her father’s alma mater has a particularly large population of students from Europe, so she accesses the institution’s website. She notices right away that the content is translated into a number of languages, including Spanish and French. Lucia uses a web-based chat interface to ask questions of a representative of the admissions office at her father’s alma mater. During the course of that conversation, Lucia shares information about her school grades and hobbies. She also inquires about scholarships and whether she could receive discounted tuition since her father is an alum. Finally, she asks whether the institution offers special services to students with disabilities. Several days later, Lucia receives postal mail from the institution, with numerous brochures telling her about the institution and its programs and services for students.

Ultimately, Lucia decides to stay in Spain and attend college in Barcelona. She remembers her internet-based chat conversation with her father’s US-based alma mater and worries that she shared too much personal information. She contacts the admissions office and asks that the institution delete all of the personal data that she shared during her chat conversation. She asserts that she has the right to be forgotten under European Union law and that the US institution must comply.

1 What is it?
The General Data Protection Regulation (GDPR) was approved by the European Union (EU) in April 2016. It comes into force on May 25, 2018. GDPR requires that covered organizations put significant processes and safeguards into place regarding the collection, use, and processing of personal data of data subjects located in the EU. GDPR uses several defined terms of art that have special meaning within the regulation. A data subject is an identified or identifiable natural person. Personal data are any information about an identified or identifiable data subject, which can include direct identifiers, such as name, address, email address, and national identification numbers, or indirect identifiers such as location data or IP address. This list of data elements is not exhaustive, and the definition of personal data under GDPR should be considered in the broadest possible context.

2 How does it work?
GDPR does two things: It explicitly confers numerous rights on data subjects who are located in the EU, and it requires covered organizations to put significant processes and safeguards into place regarding the use and processing of the personal data of those data subjects. The rights that GDPR confers on individuals are numerous. Some (but not all) of these protections include an individual’s right to access any data that an organization has collected about that person; the right to know why an organization is processing that person’s personal data and the categories of personal data that an organization processes; the right to correct any errors in personal data collected or processed; and the right to know how long an organization will store the individual’s personal data. One of the most novel protections is known as the right to be forgotten or the right to erasure. This means that, under certain circumstances, an individual can require an organization to permanently delete any of that individual’s personal data.

Similarly, GDPR imposes a number of obligations on the organizations that are subject to it. Some (but not all) of these requirements mandate that an organization have a legal basis for collecting and processing the personal data of EU data subjects, document that legal basis, and only collect and use data when a legal basis exists; minimize the collection and processing of personal data whenever possible; protect any collected personal data; assess risks related to collecting and processing the personal data of EU data subjects and implement a plan to mitigate those risks.
GDPR

and impacts; and have a breach notification policy and notify authorities within 72 hours of learning of a breach. In some instances, GDPR also requires that some organizations appoint a data protection officer (also referred to as a DPO) to oversee the organization’s data processing operations.

3 Who’s doing it?

The EU has long viewed data privacy as a fundamental human right. It issued its first data privacy directive in 1995, which EU member states were free to adopt and incorporate into their own national state laws. Unlike the 1995 effort, the GDPR is a regulation that applies its protections across EU member states directly without requiring adoption by individual nations. Organizations in the EU must comply with the GDPR. In addition, organizations (regardless of where they are located) that offer goods or services to people in the EU or that collect data on people located in the EU also must follow GDPR. Since organizations both inside and outside the EU may have to comply with the GDPR, this expansive scope is sometimes considered the “borderless” application of GDPR. For its enumerated data privacy protections, GDPR applies to EU data subjects regardless of their citizenship or nationality. Much like an American in Paris would need to follow Paris traffic regulations, that same American’s personal data would be protected by the GDPR while in France. This is the concept of territoriality—GDPR protects all data subjects within EU borders.

4 Why is it significant?

Failure to comply with GDPR can result in an enforcement action and significant financial penalties. In addition, due to both the borderless application of GDPR and the concept of territoriality, the regulation has broad implications for organizations around the globe, including US colleges and universities.

5 What are the downsides?

Although organizations have had almost two years to prepare for GDPR, which was approved in 2016, the regulation’s expansive requirements and protections and its potentially expansive application have left many organizations struggling to achieve compliance. Organizations that are not located in the EU, have few business relationships in the EU, or only have a web presence accessible in the EU have grappled with whether the GDPR applies to their data collection activities. In other instances, organizations have understood the GDPR to be a regulation that addresses data protection only and have tasked IT departments with ensuring GDPR compliance. This approach may not be enough to ensure GDPR compliance. Although GDPR has some provisions that may call into question how data in IT systems are used and secured, practically speaking it looks at all aspects of how organizations use and collect data from EU data subjects.

6 Where is it going?

The GDPR is a complicated piece of legislation, and many of its impacts will not be fully understood until after the May 2018 enforcement date. As individuals around the globe become aware of GDPR, organizations everywhere can expect their constituents to be aware of the law and potentially interested in asserting their data privacy rights. Organizations that can demonstrate compliance with GDPR’s requirements could have a competitive advantage in the global marketplace among consumers who are interested in protecting their personal data.

7 What are the implications for higher education?

GDPR may pose a concern for US higher education institutions. Examples of potential interactions that may involve the collection and use of the personal data of EU data subjects include student recruitment and admissions activities, study-abroad programs, faculty and staff recruitment, and international research activities. These interactions must be fully understood, documented, and assessed for GDPR applicability. To properly assess the impact of GDPR, numerous institutional stakeholders, from legal counsel to business unit directors to data stewards to IT organizations, must work together to understand the rights and obligations conferred by the GDPR and how the institution collects and uses data from EU data subjects. These same stakeholders must also work together to understand the business risk that GDPR noncompliance introduces and how best to mitigate that risk within the context of all other institutional business risk.

This EDUCAUSE 7 Things resource does not constitute legal advice. Institutions are strongly encouraged to consult with their legal counsel to understand the application of GDPR, if any, to institutional data collection activities. See EU General Data Protection Regulation (GDPR) for more information and resources.