# THE GENERAL DATA PROTECTION REGULATION

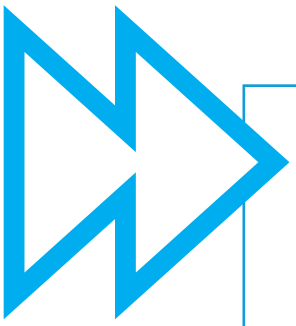
## Analysis and Guidance for US Higher Education Institutions

**Author:** Dr. Gabriela Zanfir-Fortuna,
*Senior Counsel, Future of Privacy Forum*

**Editor:** Ashleigh Imus

FUTURE OF PRIVACY FORUM

MAY 2020



This guide is intended to help US-based higher-education institutions and their edtech service providers analyze and comply with Europe's comprehensive data protection and privacy law, the General Data Protection Regulation (GDPR). When the GDPR came into effect, there was limited guidance and decisions available to help US higher education institutions and edtech companies in understanding their obligations. Now, two years into the regulation's implementation, there is significant guidance that can be analyzed and applied. Colleges should assess their GDPR compliance if they accept applications from EU residents, provide online classes to individuals in the EU, operate study abroad programs in the EU, interact with EU-based alumni, or otherwise collect or use data about people in the EU. Edtech companies should also assess their GDPR compliance if they provide services, directly or as a vendor to a college, to people in the EU. This guide does not provide legal advice but is meant to support compliance efforts and to advance legal assessments.


# INTRODUCTION TO THE GENERAL DATA PROTECTION REGULATION

The GDPR is the common name for *Regulation (EC) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*.[1] The law was adopted on April 27, 2016, after four years of legislative process, and went into effect on May 25, 2018. The regulation updates and repeals a longstanding personal-data protection directive, Directive 95/46, but maintains and details most of the concepts, rights, and obligations provided in that directive.

The GDPR gives individuals certain rights to control how their personal data is collected and used. The law provides a high level of protection for individuals whose personal data is collected because the EU member states recognize personal-data protection as a fundamental right, separate from the right to privacy (even if connected to it), as described in Article 8 of the EU Charter of Fundamental Rights.

To provide these rights, the law operationalizes data protection by detailing the ways in which individuals may exercise their rights, and grants them a private right of action. It also establishes avenues to ensure accountability for organizations that process personal data subject to the law, specifically legal obligations and significant sanctions for non-compliance. This means that organizations need to determine whether the GDPR applies to their data-processing activities and, if so, to establish compliance practices. The GDPR lays out fundamental principles that inform its requirements for the treatment of personal data. These principles include lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. In the following sections, we discuss how these principles function in practice. Specifically, we explain the circumstances in which the rights of data subjects intersect with data-processing activities commonly conducted by US higher-education institutions and their edtech service providers.

In Part I, we introduce the scope of the GDPR's application and briefly relate it to common data practices of higher-education and edtech organizations. In Part II, we outline ten steps that institutions should take to establish their GDPR compliance programs, and explain how organizations can follow each of the ten steps. Here, we offer detailed information on the GDPR's definitions and requirements, and we contextualize this information in terms of many of the data-processing activities that require US higher-education institutions and edtech service providers to comply with the law.

The following content should be deemed not legal advice but mere guidance to safely navigate the complexity of GDPR compliance.

# PART I: GDPR SCOPE OF APPLICATION

In outlining its scope of application, the GDPR uses the terms "personal data," "data subjects," "controller," "processor," and "processing." We thus briefly introduce these concepts here and explain them in further detail in Part II (Step 9). According to the GDPR, anything that can be done to personal data counts as processing (e.g., collection, recording, organization, structuring, storage, dissemination, and so forth). A controller is the entity that alone or jointly with others establishes the means and purposes of processing. A controller can be an individual or an organization. A processor is an entity that processes personal data on behalf of a controller.

Most of the GDPR's statutory obligations are directed at controllers. Controllers are the parties responsible for ensuring that the processing of personal data complies with all of the regulation's data protection principles. In addition, controllers must perform due diligence when hiring vendors (processors) to process personal data on their behalf.

For the GDPR to apply, an act of data processing must be subject to the law in all three of the following categories: the material scope (what), the personal scope (who), and the territorial scope (where).

## MATERIAL SCOPE: To What Does the GDPR Apply?

The GDPR applies to the processing of "personal data," which is the legal term used in EU data protection and privacy law, in contrast to the terms "personal information" or "personally identifiable information" used in US laws. Personal data is a broad concept under the GDPR and includes more than what is commonly understood as personally identifiable information.

The GDPR legally defines personal data as "any information relating to an identified or identifiable natural person" (Article 4.1 GDPR). The phrase "any information" reflects the EU legislature's aim to assign a broad scope to that concept. The concept is not restricted to information that is sensitive or private, and potentially encompasses all kinds of information, both objective and subjective, in the form of opinions and assessments, provided that it *relates* to the data subject.[2] The concept also includes publicly available information, to which the law offers protection equal to what it provides for all other personal data.

For example, in several cases in the EU Court of Justice, the following information relevant to higher-education institutions' activity has been found to be personal data: written answers submitted by a candidate on a professional examination; any comments made by an examiner regarding written answers submitted by a candidate on a professional examination; handwriting; information related to salaries/remuneration; amounts of subsidies received; amounts of earned or unearned income and assets of natural persons; information about daily work periods, rest periods, and corresponding breaks and intervals; working conditions and hobbies; internet protocol (IP) addresses; dynamic IP addresses; image of a person recorded by a camera.

The GDPR applies to all processing of personal data as long as it is not conducted by a law enforcement agency of an EU member state; it is not conducted in the national security interest of a member state; it is not conducted for purely personal or household purposes; or it is not conducted by an EU institution or body.

The GDPR has a different application compared to that of the Family Educational Rights and Privacy Act (FERPA). FERPA applies to the use of student records. In contrast, the GDPR applies to all processing of personal data by education institutions. In certain situations, this may include not only data collected in student records but also metadata regarding how students interact with digital courses and homework (even if simply a unique cookie ID or an IP address), video surveillance (CCTV) monitoring on campus, HR-related data about staff, application forms, and marketing activities, among other things.
See Part II of this guide for more details on the material scope of the law.

## PERSONAL SCOPE:
## To Whom Does the GDPR Apply?

The GDPR is designed to protect data subjects. A data subject is the person whose data is processed. To be protected by the GDPR, the data subject must be an individual who is a living natural person. The data subject can be an identified individual or an identifiable individual. The GDPR defines an identifiable natural person as one "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4.1 GDPR).

The GDPR does not contain any citizenship, nationality, residence, or legal status conditions for an individual's protection by the regulation. The only condition on the GDPR's application to an individual's personal data is that the individual must be alive. Note that legal persons (i.e., organizations) are not protected by the GDPR.

A campus in the EU must apply data protection rules to all its enrolled students, faculty, and staff, regardless of their nationality and of where they are based (including, for example, long-distance students based outside the EU in the US). The GDPR likely applies to students enrolled in a US education program who are participating in a semester abroad program in an EU member state if the semester abroad involves "offering a service" to these students while they are in the EU.

Part II of this guide offers further details on the personal scope of the GDPR.

## TERRITORIAL SCOPE:
## Where Does the GDPR Apply?

The GDPR applies to the processing of personal data conducted through the establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the EU. The term "establishment" has been construed broadly in past cases. This means that the GDPR applies to the processing of personal data as part of activities of campuses in the EU, admission offices in the EU, branch research institutes in the EU, and any institutes in the EU that have a sufficient degree of stability. If an institution has an office in the EU or a personal representative engaged in the institution's core activity, then the GDPR applies to all personal data in the context of that presence in the EU.

Even if the institution does not have a presence in the EU (such as an office or campus), the GDPR might still apply if a US-based institution provides services or goods to natural persons physically in the EU or if it monitors the behavior of natural persons in the EU. For example, if an institution has an online educational course with registrants from the EU, the GDPR would likely apply to the processing of personal data in that context. If the institution collects and processes the personal data of data subjects in the EU in the admissions process, the GDPR likely applies to that processing. If the institution maintains relationships with alumni based in the EU, the GDPR also likely applies.

The European Data Protection Board (EDPB), which determines the GDPR's application, has specified that certain types of targeting of goods and services to EU persons triggers the application of the GDPR to organizations outside the EU. See Part II of this guide for further information on those elements related to activities of higher-education institutions.

If an institution monitors the behavior of data subjects while they are in the EU, the GDPR applies to such monitoring. The GDPR may also apply to research conducted in the EU or that includes subjects who are in the EU if the research involves monitoring their behavior. The law would also likely apply to research conducted in the US that involves the personal data of non-EU residents, but is done on behalf and at the direction of an organization established in the EU. In this case, the research center or institution in the US is likely a processor for the organization in the EU, which is a controller and is therefore responsible for how it processes

personal data and for how its processors do so. In this case, the US institution would need to enter a controller-processor agreement with the EU organization and comply with the EU organization's instructions (see Part II of this guide for further information about such agreements).

These two extra-territorial conditions, regarding the provision of goods and services and monitoring behavior, were introduced by the GDPR and do not have an equivalent in past legislation. Therefore, no practices or case law exist that organizations can use to determine whether either situation applies to them.

The GDPR does not likely apply to the processing of personal data that occurs while students originating in the EU are physically on campus in the US. Examples of such processing while on campus in the US might include CCTV images, information regarding the use of library cards, evaluations and grades, and monitoring of students' assignments. Part II describes the territorial scope of the law in further detail.

Note that according to the EU-UK Brexit deal, the UK is currently in a transition period that will end on December 31, 2020, unless it is prolonged. During this transition period, the GDPR will continue to apply in the UK as if the UK were still a member state, even if the UK Data Protection Authority (the Information Commissioner's Office) will not be a member of the European Data Protection Board. During the transition period, the EU and the UK will further negotiate whether the GDPR will apply and, if so, how it will apply once the transition is over.

## PART II: TEN PRACTICAL STEPS TO BEGIN A GDPR COMPLIANCE PROGRAM

GDPR compliance is a substantial, complex, and ongoing process. It typically requires determination and resources, especially human resources and time. To facilitate this process, this section of the guide proposes ten steps for initiating a solid GDPR compliance program in higher-education institutions and other relevant organizations. The subsequent section describes how to carry out these steps.

**Step 1.** Assign Responsibilities.

**Step 2.** Identify Data Flows That Are Subject to the GDPR.

**Step 3.** Identify Data Flows That Qualify as International Data Transfers, and Establish a GDPR-Compliant Mechanism for Each Transfer.

**Step 4.** Document the Lawful Grounds That Support the Institution's Data-Processing Activities.

**Step 5.** Create a Register of Processing Activities.

**Step 6.** Understand the Rights of Data Subjects Under the GDPR, and Set Up an Internal Process to Address Requests.

**Step 7.** Establish a Retention Schedule for the Personal Data That Is Subject to the GDPR.

**Step 8.** Adopt a General Privacy Policy That Is GDPR-Compliant, and Establish the Specific Privacy Notices that Are Necessary.

**Step 9.** Identify All of the Organization's Data Processors, and Establish Controller-Processor Agreements With Them.

**Step 10.** Implement Technical and Organizational Data Security Measures.

Here we describe how to enact the ten steps outlined above, including detailed information on some of the requirements for GDPR compliance in terms of data-processing activities in which higher-education institutions and edtech companies frequently engage. At the end of this section, we also describe the sanctions for noncompliance with the GDPR.

## STEP 1: Assign Responsibilities.

Organizations should designate either an individual or a team to coordinate the GDPR compliance program. The organization will also need to determine whether it is obliged to appoint a data protection officer (DPO) and a legal representative in the European Union.

GDPR compliance, as well as the reputational and financial risks of noncompliance, should be brought to the attention of the president, Board of Regents, or whichever individual or board represents the highest management level of the institution. This will ensure that sufficient human and financial resources are allocated for GDPR compliance efforts and that the institution will be ready to make operational decisions about the processing of personal data subject to the GDPR. Some of these operational decisions include enhancing transparency, publishing new GDPR compliance notices on how personal data is processed, and asking all vendors that have access to GDPR data to enter controller-processor agreements.

If the institution has appointed a chief privacy officer (CPO), that individual, along with his or her team, should be at the center of GDPR compliance

efforts. Other parties who should be involved in GDPR compliance efforts include the office of the general counsel and representatives of the team that manages IT infrastructure and security.

Responsibility for GDPR compliance should be assigned to an individual or team; this individual or team should convene a task force to create a central point of communication for all offices or departments that may be affected by the GDPR. This task force will help the institution understand which data it collects, how it is being used, and the most effective way to provide notice to affected parties.

**Criteria for appointing a data protection officer**. All institutions that collect and use data covered by the GDPR may appoint a DPO, and some entities must do so under the law. The DPO monitors compliance with the GDPR, provides advice to the institution, supports the development of policies and procedures that facilitate responses to GDPR-related requests, and serves as a point of contact for data subjects and supervisory authorities. Although DPOs cannot make decisions regarding the means and processing of personal data, they can provide advice to the decision makers.

According to the GDPR, organizations processing personal data, regardless of whether they act as controllers, joint controllers, or processors, must appoint a DPO if at least one of the following three criteria applies:

1. The processing is carried out by a public authority or body that is recognized as such under EU or member-state law;
2. The core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale;
3. The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses (Article 37.1.a–c GDPR).

The first requirement applies only to organizations established or recognized as a public authority or body by the EU or its member states. This means that very few higher-education institutions will be required to appoint a DPO under this criterion.

The second requirement is much more expansive and covers any organization conducting large-scale monitoring of persons. For example, if the institution has a campus in the EU and uses learning analytics on the entire student body enrolled on that campus, the processing will likely be considered large-scale monitoring of data subjects. However, an institution that conducts large-scale learning analytics at a campus in the US would probably not be required to appoint a DPO, because those processing activities are not regulated under the GDPR.

The third requirement involves the large-scale processing of "special categories of data," which include health data (see Step 2 below for more on special categories of data). A university hospital will inevitably process special categories of data on a large scale, but if that university hospital is not in the territory of the EU, its processing activities are not subject to the GDPR, so no DPO is required. The GDPR could apply in this scenario if patients based in the EU receive remote medical advice or remote treatment while they are physically in the EU. However, such instances will likely not occur on a large scale and therefore will not require the appointment of a DPO.

It is unlikely that many US-based educational institutions will be obliged to appoint a DPO. However, this depends on the circumstances of each institution, particularly whether the institution has a campus in the EU. All institutions that process personal data subject to the GDPR should conduct a formal assessment to determine whether they need to appoint a DPO. The assessment should be kept as a record of accountability. Institutions not obligated to appoint a DPO can still do so, to support and monitor GDPR compliance efforts and to facilitate dialogue with data subjects and supervisory authorities as necessary. Appointing a voluntary DPO will likely be considered a sign of good faith.

## STEP 2: Identify Data Flows That Are Subject to the GDPR.

This section is the most extensive of Part II because higher-education institutions and edtech companies engage in many data-processing activities, and these organizations also need to understand how the GDPR classifies types of data. We first explain types of data according to the GDPR and then address categories of activities that are likely subject to the law.

As noted in Part I, the GDPR applies to "personal data" and defines such data in broad terms. The law also defines special categories of data that are subject to special protection.

**Special categories of data**. Article 9 of the GDPR describes these special categories of data. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning an individual's sex life or sexual orientation.

The GDPR includes a general prohibition against the processing of special categories of personal data unless it is for one of the following permissible uses:

- **Explicit consent** of the data subject;
- **Employment and social security law:** to carry out obligations under employment and social security protection law (if authorized by law or by a collective agreement);
- **Vital interests**: to protect the vital interests of the data subject or of another person;
- **Political/religious not-for-profits:** the processing is carried out with appropriate safeguards by a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim, and on condition that the processing relates solely to the members or former members of the body or to persons who have regular contact with it and that the personal data is not disclosed outside that body without consent;
- **Data manifestly made public:** the processing relates to personal data that is manifestly made public by the data subject;
- **Legal claims:** to establish, exercise, or defend legal claims;
- **Substantial public interest:** for reasons of substantial public interest, on the basis of union or member-state law;
- **Medical purposes:** for the purposes of preventive or occupational medicine, to assess the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, the management of health, social care systems, and services on the basis of union or member-state law, or pursuant to a contract with a health professional;
- **Public health:** for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of union or member-state law;
- **Archiving, scientific, or historical research:** for reasons of public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) GDPR based on union or member-state law. For data related to health, the Court of Justice of the European Union decided that this notion must be given a wide interpretation so as to include all aspects, both physical and mental, of the health of an individual. The GDPR defines "genetic data" as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question" Article 4.13 GDPR).

**Key-coded data**. Some organizations use key-coded (i.e., masked or pseudonymized) data in their processing activities. The GDPR includes the concept of key-coded data in its protection of personal data, so key-coded data is also subject to the GDPR. Specifically, under the GDPR, personal data that has undergone a pseudonymization process remains personal data as long as the key exists and can re-identify the data set. Such personal data is considered to be information about an identifiable natural person.Next, we discuss common higher-education and edtech data-processing activities that might be subject to the GDPR.

**Admissions**. Admissions is likely the process that the GDPR will impact most for US higher-education institutions. Below we discuss many of the situations in which US institutions need to ensure that their practices comply with the GDPR.

European residents apply directly to US higher-education institutions. As noted above, controllers who are not established in the EU are obliged to process data in accordance with the GDPR as long as the personal data pertains to individuals who are within the EU and the data is processed as part of providing goods and services or monitoring their behavior while they are in the EU (Article 3.2 GDPR). This means that the GDPR applies to the personal-data processing of data subjects who are physically in the EU, and this includes the admissions process.

However, the European Data Protection Board has indicated in official guidance[3] that an additional element of targeting EU-based individuals by offering them goods or services must be present for the GDPR to apply when the organization is based outside the EU. For example, the GDPR will apply to the admissions process if institutions do any of the following:

- Participate in any promotional events in the EU, such as higher-ed fairs;
- Include in marketing communications the email addresses, home addresses, or phone numbers of prospective students in the EU;
- Target online ads, based on relevant criteria, to prospective students in the EU.

Other elements of targeting may include accepting payments in euros or other currencies of EU member states, having EU-specific website domains (such as .de or .es), or allowing prospective students in the EU to submit materials in their native language.

Institutions will not have to change their admissions process for these applicants, but they must be transparent about practices and potentially set up new safeguards. A dedicated privacy notice for the admissions process is highly recommended, and the notice should be easily accessible and visible to all applicants.

If any automated decision-making occurs in the admissions process, this must be disclosed in the privacy notice. For example, some institutions use an automated program to pre-screen all files, to exclude applicants based on certain criteria. This kind of automated decision-making has a significant effect on individuals because it can result in a missed opportunity to receive education. Special safeguards must be in place for this kind of processing, and transparency about it is required.

Information about retention periods of personal data submitted through the application process should be established and made available to applicants. Institutions should set up processes to respond to requests from individuals who want copies of their file submitted for admission or who want to have it erased or destroyed. Note that the GDPR also applies to non-automated processing of personal data as long as it is part of a filing system. This includes paper admission forms that an institution receives.

The GDPR protections described above also apply when European students send test scores to academic institutions with the intention to support an application, even if the scores are sent in the absence of a formal application. Test

scores are considered personal data and are protected under the GDPR.

Likewise, if a European student sends personal data to an institution as part of the admissions process and then stops interacting with the institution, the data is still protected under the GDPR. This means that the data retention schedule should be applied to the data (see Step 7 for details on data retention schedules). Institutions should include this specific situation in the data retention schedule and establish a reasonable time frame in which individuals' personal data is erased after the institution's last communication with the individuals. Until these individuals' data is erased, they have the same rights under the GDPR as do all the other data subjects whose personal data is processed by the institution.

European residents move to the US to study at a higher-education institution. In this case, the GDPR compliance requirements for the institution will change. When European students are admitted and move to the US to study on campus, then the processing of their personal data on campus in the US, such as CCTV footage, grades and test scores, learning analytics patterns, and so forth, is not subject to the GDPR.

When the students move back to the EU and educational institutions process their personal data in the context of alumni relationship activities, the GDPR likely applies to that processing.

It is also possible that the GDPR would apply to student records and any other personal data stored by institutions after students move back to the EU, even if those records were created while students were physically in the US. This would mean, for example, that students would have the right to receive a copy of their records or any other personal data the institution may hold. The rationale here is that mere storage of personal data amounts to "processing" as defined by the GDPR. The storing of personal data created or collected during the studies of individuals who are in the US and then subsequently in EU territory could be interpreted as processing personal data in the context of offering educational services. This is, however, an open question and needs to be clarified by supervisory authorities or through case law.

Admissions offices buy names and contact information from a third-party vendor. In this situation, institutions need to ensure GDPR compliance if the lists include EU persons. Email marketing is covered by the ePrivacy legal framework in the EU (Directive 2002/58), which requires that such marketing occurs only with the consent of individuals, unless the individual and the controller are already in a business relationship for a similar product or service. The consent obtained

by the third-party vendor might be valid for the processing conducted by the institution acquiring the list if the third-party vendor, when it obtains consent from data subjects to share their contact information for marketing purposes, specifically names the institution (i.e., the data controller). This will depend on the specificity of consent obtained by the vendor.

If an institution acquires a list of contacts and does not know whether the vendor obtained consent for direct email marketing on the institution's behalf, then sending emails to require consent directly from people on the list is likely unlawful in all EU member states. For further guidance, see the ICO's guide on electronic mail marketing.[4] These rules do not apply to the processing of contact information for marketing via traditional mail, which can be based on other applicable lawful grounds. However, institutions need to allow recipients the opportunity to opt out from both email and traditional mail marketing. Institutions also must include information about this data use in their privacy notice.

Students who currently reside in the EU apply to a higher-education institution through a third-party platform. If an institution relies on a third-party platform for their admissions process, the platform likely acts as a processor, which means the platform processes applicants' data on behalf of the institution. In this case, the institution must establish a controller-processor agreement (see Step 9 for details on this).

**Learning analytics**. An institution uses a learning management system that shares enrollment information among people in the same class. In general, all processing of personal data is permitted as long as it complies with one of the GDPR's lawful grounds and the institution complies with fundamental data protection principles, such as data minimization and purpose limitation. If the processing is done only for statistical purposes, then it is likely compatible with the initial purpose for which the personal data was collected. This means that institutions would not need to justify the processing with one of the lawful grounds, but they would still need to apply all other data protection rules, such as including the processing in the privacy notice, using data protection-by-design principles when setting up the automated system, using pseudonymized or encrypted data when possible, establishing data security measures, and having processes in place to address requests from data subjects.

If the learning management system is used for purposes other than statistical ones, then the institution should assess whether the new purpose is compatible with the original one for which data was collected (in this case, enrollment).

If the purpose is compatible with the original one, then there is no need to identify a new lawful ground. If the purpose is not compatible, a new lawful ground must be documented. The institution also must determine whether the new purpose involves automated decision-making that may have a legal or significant effect on the data subject under the GDPR. The GDPR has a general prohibition against solely automated decision-making that significantly or legally affects a person, with a few exceptions (see page ____ for further details).

An institution uses a learning management system that stores evaluations, correspondence, and grades for students in the cloud. Cloud storage is permitted. If a vendor provides cloud storage as a service for an institution, then a controller-processor agreement may be necessary. The first step is to determine whether the GDPR applies to the specific processing operation that required information storage in the cloud. If that processing involves data collected from students while they are in the US, the GDPR probably does not apply to that data. The answer depends on the context and specificities of the processing activity. Another important aspect of compliance in this context is to ensure that the processor (vendor) has sufficient data security, technical, and organizational measures in place.

An institution restricts educational opportunities based on outcomes from a learning analytics system. If the GDPR applies to the personal data that serves as input to the learning analytics system, the institution must comply with the GDPR provisions on profiling and automated decision-making. Therefore, it is very important to first establish whether the GDPR applies to the processing of the personal data at issue.

The GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements" (Article 4.4). If an institution uses any data processing to make inferences about their student(s), even if it does not result in a decision regarding the student(s), it is still considered profiling and requires additional documentation. Institutions will likely need to conduct a data protection impact assessment (Article 35.3.a; see Step 10 in this guide) to determine the risks to individuals' rights and interests and to propose measures to mitigate the risks.
If this kind of processing also amounts to a solely automated decision-making process resulting in a decision that may have legal or significant effects on a student, the GDPR in principle prohibits it but allows the following exceptions. Decision-making without human involvement is permitted only if it is necessary to enter into or perform a contract with data subjects, if the EU or a member-state law authorizes it, or data subjects explicitly consent to it. Of these three permissible uses, explicit consent is the only one likely to apply in the context of learning analytics that may result in changes of instruction or class outcome. Institutions likely cannot rely on the need to perform a contract as a permissible use, because generally educational services can be provided without the use of learning analytics. It is therefore important for educational institutions to assess whether the learning analytics process has a significant effect on students.

The GDPR's transparency obligations also require that privacy notices specifically mention the existence of automated decision-making, including profiling, that is solely automated and may have legal or significant effects on individuals. The notice must also include meaningful information about how the automated processing makes decisions as well as the significance and the envisaged consequences of such processing for data subjects (Article 13.2.f).

If a vendor provides the learning management system, the institution must establish a controller-processor agreement (see Step 9).

The European Data Protection Board has published guidelines[5] that offer further information

on automated individual decision-making and profiling under the GDPR.

**Intra-institutional data sharing.** The GDPR allows institutions to share information within departments (e.g., admissions shares data with the financial aid department), but this sharing must not violate the GDPR's purpose-limitation principle (Article 5.1.b). This rule states that personal data must be processed only for the specified purpose(s) for which they were collected and must not be further processed in a manner incompatible with that purpose(s).

For example, if an institution collected personal data of prospective students for the purpose of admissions, it cannot then process that data to advertise sporting events organized by teams unless the institution has in place a lawful ground for the new purpose and informs data subjects about it.

To determine whether a new purpose is compatible with an initial purpose for processing, controllers must consider the following:

- Links between the purposes for which the personal data was originally collected and the subsequent purposes of further processing. For example, there is a reasonable link between admissions and student aid if applicants request student aid as part of their admissions process;
- The context in which the personal data was collected, particularly the relationship between data subjects and the controller;
- The nature of the personal data, particularly whether special categories of personal data are processed;
- The possible consequences for data subjects, resulting from the additional processing;
- The existence of appropriate safeguards, which may include encryption or pseudonymization.

Note that the GDPR considers additional data-processing activities for archiving purposes in the public interest, for scientific or historical research purposes, and for statistical purposes to be compatible with the initial purpose for which the data was collected. This means, for example, that data related to admissions may be shared with the department that coordinates statistics without the need to establish a new lawful ground for processing (such as obtaining consent). However, such additional processing is still subject to transparency obligations, such as inclusion in the privacy notice, and other safeguards.

**Online classes**. If a student in Europe takes an online class and the applicability conditions discussed above in Step 1 are met, the GDPR applies to all processing of personal data that occurs in the context of providing the online course, not only to admissions or enrollment in that course. Among the important steps that institutions should take are the following:

- Specific notice must be given to the student;
- A lawful ground as defined by the GDPR must be present for all processing activities that occur in this context (see Step 4); for example, if metadata and engagement data related to the course are used for purposes other than providing the course, such as profiling for advertising, this purpose must be justified by a specific, individual lawful ground distinct from that which justifies the processing for the purpose of providing the service;
- The institution must establish technical and organizational measures to ensure data security and to prevent personal-data breaches;
- The institution must establish clear procedures for responding to requests related to data subjects' rights;
- The institution must incorporate data protection by design in the design of the online course and throughout the provision of the course when technical adjustments are made;
- If the online class uses cookies or similar technologies placed on the device(s) of the student, then the ePrivacy framework applies

to the placing of such technology. To place non-essential cookies (meaning cookies that are not necessary for the functioning of the website) or similar technology on the devices of students, institutions must obtain consent for all such technologies that are not essential to providing the service. If a student does not agree to the placing of non-essential cookies or similar technologies, then they must not be placed on the device.

**Semester abroad.** Subject to further guidance and case law, the GDPR likely applies to the processing of personal data by the home institution of an American student participating in a semester abroad in Europe because the student is physically in the EU and the US-based institution provides services to the student. The GDPR also applies to data processing carried out by the host EU institution.

When US colleges establish agreements with partners in the EU for exchange programs, a good practice is to include joint controllership clauses regarding the sharing of responsibility for the processing of exchange students' personal data. This is a good practice because, depending on the partnership details, the law may consider partners in exchange programs to be joint controllers, and clearly defining the extent to which each institution is responsible for the processing is both useful and mandated by the GDPR (Article 26). Joint controllership occurs when two or more controllers jointly determine the purposes and means of processing. As joint controllers, they must determine their respective responsibilities in a transparent manner, particularly regarding responsibilities for students' exercise of their rights as data subjects.

When European students come for a semester in the US, all processing of personal data by the US institution while the student is still in the EU and preparing for the visit abroad is likely subject to the GDPR. Institutions may still be joint controllers in this situation. As discussed above, the GDPR likely does not apply to the processing of personal data that occurs while students originating in the EU are physically on campus in the US.

**Alumni**. For alumni who reside in the EU, the processing of personal data for the purposes of fundraising and to offer other alumni services likely falls under the GDPR, especially if the institution has registered the alumni as based in the EU. Institutions likely do not need to change how they fundraise with alumni who reside in the EU, but they need to ensure that certain practices are in place. Institutions need to include this kind of processing in their register of processing activities; establish lawful grounds for processing; provide transparency regarding the way they process the personal data of alumni (include details in a more general privacy notice/policy or draft a separate privacy notice); and set up internal processes to reply to requests from data subjects.

Some institutions have alumni foundations that raise funds for the institution. Institutions can share graduate information with the foundation under certain conditions. If the alumni foundation has its own legal personality and is a self-standing entity (distinct from the educational institution), it could be considered a processor acting on a university's behalf when it uses graduate information to contact alumni based in the EU. This means that a controller-processor agreement should be established before the data is shared with the foundation.

If the alumni foundation is legally a part of the educational institution, a controller-processor agreement will not need to be established. Since alumni have a standing relationship with the educational institution, educational institutions can contact them through email marketing for fundraising purposes under the "soft opt-in" rule, which does not require separate consent for the communication but does require that the sender provide a clear and easy way to opt out. The UK's ICO has published guidelines[6] that offer further information regarding email marketing.

**Vendors.** When a US college's vendors perform services for the collection, storage, or

manipulation of data that is subject to the GDPR, higher-education institutions need to ensure that their vendors' data-processing activities comply with the GDPR.

For those vendors, the GDPR requires a written agreement that includes the following information (Article 28):

- The subject matter, duration, nature, and purpose of the data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed;
- The obligations and rights of the controller (the higher-education institution).

The institution's vendors must also obtain written agreement from the institution to work with third-party contractors who are involved in the processing of the relevant personal data. For a more detailed discussion of this controller-processor relationship, see "A Practical Guide to Data Controller to Data Processor Contracts under the GDPR," published by the Irish Data Protection Commissioner.[7]

Once organizations understand which activities are subject to the GDPR, they need to identify the departments and faculty involved in those activities. One way to do this is to send a survey to all faculty and departments to determine whether they process personal data originating in the EU.

## STEP 3: Identify Data Flows That Qualify as International Data Transfers, and Establish a GDPR-Compliant Mechanism for Each Transfer.

Sometimes personal data transfers will happen entirely within a country; at other times, personal data moves across borders. Higher-education institutions need to know when international data transfer occurs, because the GDPR includes restrictions on such transfers. Neither the GDPR nor the previous Directive 95/46 defines an "international data transfer," but the GDPR does indicate that personal data that "moves across borders" is sufficient to constitute an international data transfer (see Recital 116).

For a transfer to be considered an international data transfer and to require the provisions outlined in Chapter V of the GDPR, the sender of the data must be in the EU and the recipient must be in a third country, which means the country is not a member of the EU or of the European Economic Area.

Examples of such a transfer may include[8]

- Sending of personal data by a controller to a non-EU recipient by post or email;
- "Push" of data from an EU data controller's database to a non-EU recipient;
- Allowing a non-EU recipient to access an EU data controller's database ("pull");
- Direct online collection of an individual's data in the EU by a non-EU controller;
- Direct online collection of an individual's data in the EU by a non-EU processor acting on behalf of an EU data controller.

For example, when a higher-education institution works with an organization in the EU to do research on human subjects, any data transferred to the institution in the US about the research subjects would be considered an international transfer of personal data. Article 45 of the GDPR requires that all transfers from the EU to a third country or to an international organization take place only if there is a mechanism for transfers in place as described in Chapter V of the GDPR.

Transfers may occur on the basis of an adequacy decision (Article 45 GDPR); on the basis of appropriate safeguards, such as administrative agreements between public authorities, binding corporate rules or standard contractual clauses, an approved code of conduct, an approved certification mechanism, ad-hoc clauses authorized by supervisory authorities (Article 46 GDPR); or derogations for specific situations (Article 49 GDPR), such as explicit consent or necessity to enter a contract.

The options for international data transfer mechanisms are limited for US-based higher-education institutions, since they cannot certify under the EU-US Privacy Shield framework. The European Commission has declared this framework to be adequate, but only entities subject to the enforcement powers of the Federal Trade Commission and the Department of Transportation can participate in it. However, US-based higher-education institutions can enter standard contractual clauses with entities that transfer personal data from the EU, can have other transfer agreements vetted by relevant supervisory authorities, or can rely on derogations, especially when receiving personal data in the US submitted by individuals. The European Data Protection Board has issued guidelines stating that derogations may be used only for specific, non-repetitive, and non-massive transfers.[9] An example for the higher-education context would be when a student transfers from a European university to an American one. An individual student's trans-Atlantic transfer is generally non-repetitive and requires the transfer of minimal information, such as grades.

However, if an American university has an ongoing relationship with the European university in question, for the purposes of a study abroad program or a research agreement requiring many students' personal data to be shared annually, a derogation under Article 49 GDPR may not

be the most appropriate ground for the transfer. In this situation, the two institutions should consider entering standard contractual clauses. Certifications and codes of conduct as transfer mechanisms have not yet been adopted, but supervisory authorities in the EU have begun to create necessary frameworks for them. Education stakeholders should follow this topic for further developments, which may indicate useful frameworks for higher education.

## STEP 4: Document the Lawful Grounds That Support the Institution's Data-Processing Activities.

After institutions have identified their data-processing activities that are subject to the GDPR, they must ensure that each of these activities is justified by one of the lawful grounds allowed by the law. The GDPR provides six lawful grounds that justify such processing: consent, performance of a contract, legal obligation, vital interests, public interest, and legitimate interests.

Controllers established outside the EU, including higher-education institutions, are most likely to rely on four of these legitimate grounds:

- Consent;
- Contractual necessity (entry or performance);
- Legitimate interests;
- A vital interest of the data subject or of someone else.

**Consent.** Institutions do not need to obtain consent for everything, but certain activities will always require consent. These include placing cookies on the devices of website visitors from the EU; sending email marketing communications to persons in the EU; and sending newsletters to persons in the EU. Institutions also need to establish a system for recording consent records if they rely on consent as a lawful ground. For further guidance, the European Data Protection Board released guidelines in 2018 on consent under the GDPR.[10]

**Contractual necessity**. The need to enter a contract with the data subject provides the legal ground for collecting and processing most of the personal data involved in admissions applications. This means that institutions do not need to obtain consent from applicants to process their data as part of the admissions procedure.

However, as noted above in the section on data flows, the GDPR treats special categories of data differently, such as data related to health, ethnic origin, or religious beliefs. These types of data can be processed only by relying on data subjects' explicit consent in this context; therefore, it is highly recommended that applicants not be required to provide such details in order to submit their applications. They should be given the choice to provide it, clearly indicated at the top of an application section requesting sensitive information, where they can indicate whether they consent to the collection and use of this information for admission purposes.

For further guidance, see the European Data Protection Board's 2019 guidelines on relying on a contract as a lawful ground.[11]

**Legitimate interests**. Institutions may have processing activities for which they can rely on their own or a third party's legitimate interests to process personal data subject to the GDPR. For example, a legitimate interest could involve a higher-education institution maintaining a specific directory of former graduate students who may be contacted for future research or teaching positions. To rely on legitimate interests, institutions must conduct a "legitimate interests assessment" that achieves the following objectives:

- Frames the legitimate interest pursued in specific terms, ensuring that the interest is present, real, and does not breach the law;

- Assesses the need for the personal data items processed for that legitimate interest, considering that only the data necessary to achieve the interest should be processed;
- Balances the rights of data subjects and the legitimate interests pursued. This analysis considers whether data subjects reasonably expect the processing that occurs; the impact, if any, of the processing on the data subjects; and any safeguards initiated by the institution to ensure that the processing is fair for the data subjects. If this balancing test shows that data subjects' rights do not outweigh the legitimate interests at stake, then the personal data can be processed without consent.

Even when the processing is based on legitimate interests, institutions still must inform data subjects that the processing is taking place, and must give them the chance to opt out of the processing. Institutions must also draft and keep records of a legitimate interests assessment that justifies the organization's reliance on legitimate interests. For further guidance, the Article 29 Working Party (the organization preceding the European Data Protection Board) released guidelines in 2014 on the use of legitimate interests.[12] While the EDPB has not officially endorsed these guidelines given that they were adopted under the pre-GDPR legal framework, they remain relevant because the GDPR has not modified the rules for legitimate interests. The Future of Privacy Forum-Nymity Report on practical cases regarding the use of legitimate interests offers further details on this issue.[13]

## STEP 5: Create a Register of Processing Activities.

Once organizations have determined which processing activities are subject to the GDPR, they need to create a register of processing activities. The register of processing activities is a list of all of an organization's processing activities that are subject to the GDPR, regardless of whether that organization is controller or processor. For organizations based in the US, only processing activities that are fully or partially subject to the GDPR must be recorded in the register.

The register is regulated by Article 30 GDPR and is compulsory for all processors and controllers that have more than 250 employees. Processors and controllers that have fewer than 250 employees must keep a register only for those GDPR processing activities that are not occasional, that result in a risk to the rights of individuals, or that involve the processing of special categories of data or personal data relating to criminal convictions.

The register kept by a controller organization must include the following information:

- Information about the controller, the controller's legal representative in the EU, joint controller if relevant, and DPO if relevant;
- The purpose of the processing;
- The categories of personal data and of the data subjects concerned;
- The categories of recipients of personal data (including processors but also third parties);
- Information about the existence of international data transfers and the safeguards in place;
- Data retention time limits;
- A general description of the technical and organizational (data security) measures in place.

Processors need to include a more limited list of information categories in the register:

- Information about the processor, each controller for which the processor provides data-processing services, the processor's representative, and DPO if relevant;

- The categories of processing conducted for each controller;
- Information about the existence of international data transfers and the safeguards in place;
- A general description of the technical and organizational (data security) measures in place.

As a best practice, the register should be updated regularly so that it always reflects the organization's data practices. Even if the GDPR does not require it, it is also useful to include in the register information about the lawful ground for each processing, including additional information such as links or references to legitimate interest assessments.


## STEP 6: Understand the Rights of Data Subjects Under the GDPR, and Set Up an Internal Process to Address Requests.

The GDPR grants specific rights to data subjects vis-à-vis controllers. Chapter III Articles 12–23 detail these rights, which include the following:

- The right to information, such as information about the controller, the purposes of processing, the data protection officer, and so forth (Articles 13 and 14);
- The right to receive confirmation that personal data is being processed;
- Details about the processing and a copy of the personal data being processed (Article 15);
- The right to have their personal data rectified or completed (Article 16);
- The right to have their data erased if certain conditions are met (Article 17);
- The right to restrict the processing of personal data (Article 18);
- The right to have the controller notify all recipients of their data on successful erasure, rectification, and restriction requests (Article 19);
- The right to obtain data portability if the processing is based on consent and a need to enter or perform a contract (Article 20);
- The right to object to processing activities if the controller does not have compelling legitimate grounds to continue the processing (Article 21.1);
- The right to object at any time to processing of personal data for direct marketing purposes (Article 21.2);

- The right not to be subject to a decision based solely on automated processing (without human intervention) that has a legal or significant effect on the individual (Article 22). As noted above regarding learning analytics, this kind of decision is allowed only on the basis of explicit consent, a need to enter or for the performance of a contract, or when a legal obligation of the controller requires it. For instance, excluding an application from a prospective student based on an entirely automated system is prohibited under this last right unless one of the three criteria noted above applies.

**Data subject access requests** (DSARs) are requests made by data subjects in the exercise of their right of access (Article 15). Data subjects have the right to receive from the controller confirmation that their personal data is processed; certain details related to the processing activity in question, such as the purpose of the processing, the categories of personal data processed, the recipients of the data, and other details (usually the details that are required for a notice); and a copy of the personal data being processed.

The GDPR indicates that the right of access should not adversely affect the rights or freedoms of others, including trade secrets, intellectual property, and particularly software copyright. However, the law states that "the result of those considerations should not be a refusal to provide all information to the data subject" (Recital 63), which means that even in these cases, at least partial access should be provided to the data subject.

In a case relevant to the education sector, the Court of Justice of the European Union decided in 2017 that written answers to an exam are personal data of the person taking the exam, and therefore they are subject to access requests if the other conditions for access are met (*Nowak*).[14] The court also decided that comments made in the margins of exams by evaluators are personal data of both the evaluators and the data subject taking the exam.

The "right to erasure" or the "right to be forgotten" is addressed in Article 17. Data subjects have the right to ask for erasure of personal data under the GDPR, but they can successfully do so only when certain conditions are met. There are six situations in which the right to erasure applies:

1. The personal data is no longer necessary for the purpose for which it was collected or otherwise processed;
2. The data subject withdraws consent (so this ground of erasure applies only to processing activities that were originally based on consent as a lawful ground);
3. The data subject objects to the processing and there is no overriding legitimate interest for continuing the processing;
4. The personal data was unlawfully processed (e.g., the data was processed without a valid legal basis);
5. The personal data must be erased in order to comply with a legal obligation;
6. The personal data is processed in relation to an offer of information-society services (i.e., online services) to a child.

Of particular relevance to the education sector, the GDPR states that the right to erasure is especially relevant when the data subject has given consent as a child, is not fully aware of the risks involved in the processing, and later wants to remove such personal data, especially on the internet (Recital 65).

These rights are not absolute. For example, an EU student requests that an institution remove grades from their record. General requests for erasure of grades will not be successful because maintaining a record of grades received by a student is an overriding legitimate interest of the educational institution. However, if a copy of those grades is published on the educational institution's intranet or on the publicly accessible internet, the student's request for erasure or destruction of those copies may be valid,

depending on the circumstances. The same rules apply to requests for erasure of personal data related to debts that students have with educational institutions.

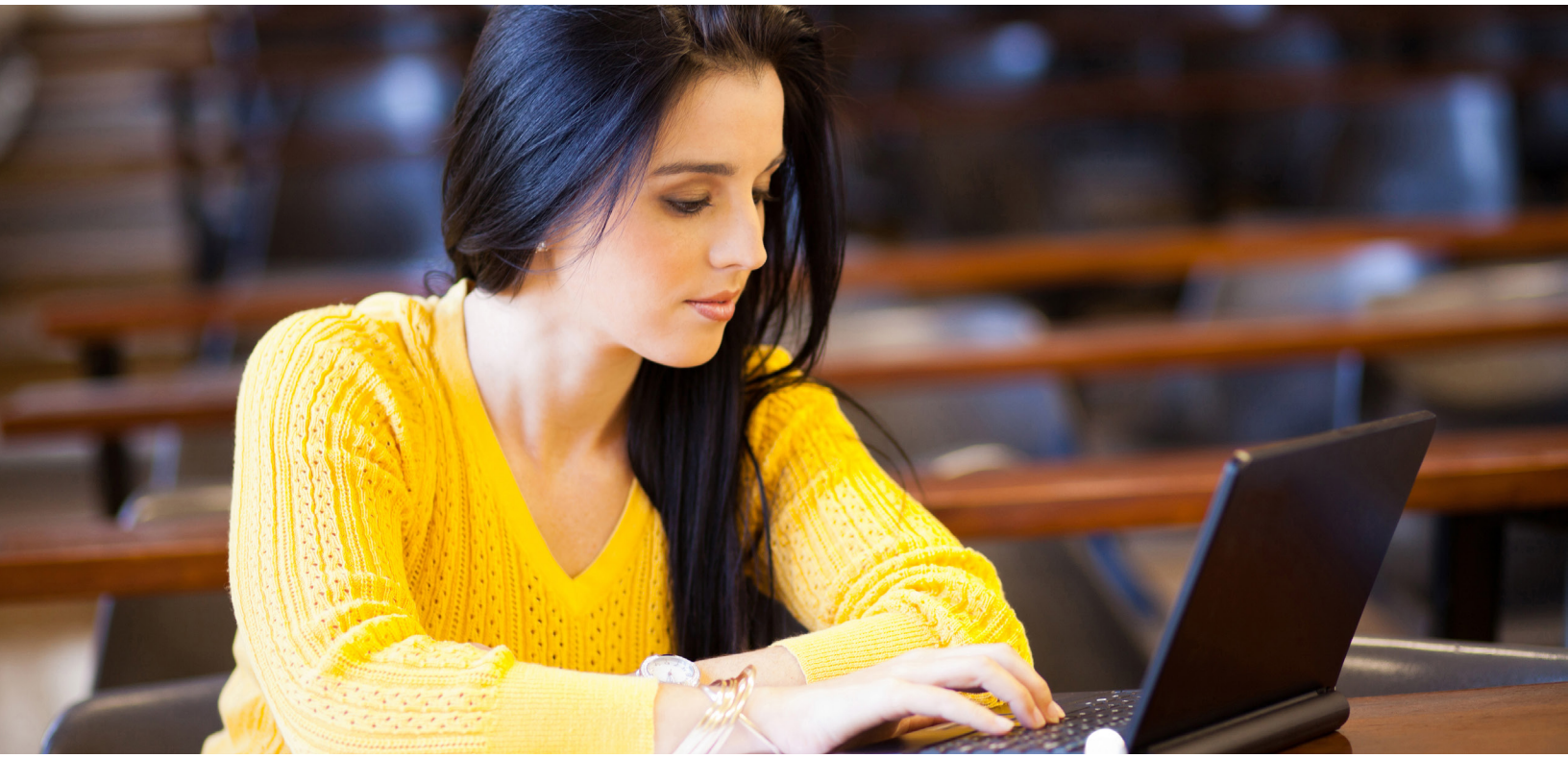
The right to erasure includes five restrictions (Article 17.3). If any of the following situations apply, an institution does not have to comply with a request to erase personal data:

1. The personal data is necessary to exercise the right of freedom of expression and information;
2. The personal data is necessary to comply with a legal obligation for the performance of a public-interest task or exercise of official authority;
   The personal data is necessary for public-health purposes in the public interest;
3. The personal data is necessary for archiving purposes in the public interest, scientific research, historical research, or statistical purposes;
4. The personal data is necessary for the exercise or defense of legal claims.

The most-relevant exceptions for higher-education institutions are likely freedom of expression and scientific or historical research. These exceptions may apply only to the extent that the personal data subject to the erasure request is necessary for these purposes. EU law interprets necessity restrictively when it impacts fundamental rights.[15]

For an erasure request, when two fundamental rights are at odds, such as the right to personal data protection and the right to freedom of expression, a balancing of the two rights is necessary before more weight is given to one or the other.

The rights of the data subject may also be restricted by member-state law for specific reasons, such as national security; defense; public security; the prevention, detection, or prosecution of criminal offenses; and the rights and freedoms of others (Article 23). Such restrictions can be found in the national laws of EU member states.



## STEP 7: Establish a Retention Schedule for the Personal Data That Is Subject to the GDPR.

Retaining all personal data indefinitely contradicts one of the fundamental principles of the GDPR: the storage limitation principle. The GDPR requires that personal data in a form allowing identification of data subjects be kept for no longer than is necessary for the institution's data-processing purposes (Article 5.1.e). Personal data may be stored for longer periods only if the data is processed for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

This means that higher-education institutions and other relevant organizations need to create a schedule that outlines how long they will retain certain categories of data. To do so, they need to determine reasonable time frames necessary to retain specific categories of personal data to achieve the purpose for which the data was collected and processed. For example, admission materials of unsuccessful applicants could be kept only as long as those students can challenge the institution's decision not to admit.

When establishing retention periods, institutions should also incorporate legal obligations, statutes of limitations, and other legitimate reasons requiring controllers to keep personal data.

## STEP 8: Adopt a General Privacy Policy That Is GDPR-Compliant, and Establish the Specific Privacy Notices That Are Necessary.

Transparency is another key principle of the GDPR, which requires that data subjects be informed in a timely, accessible, and easily understandable manner, in clear and plain language, about the fact that their personal data is being processed. The right to receive information about data processing is very important in the GDPR framework because it facilitates the exercise of the data subject's other rights.

Organizations that process personal data subject to the GDPR are therefore required to have privacy policies. Moreover, organizations must inform data subjects about the details of the processing activity, regardless of whether the data is collected directly from the data subject or from third parties. Notification must include, among other required details, the purpose of the data processing, the recipients of the personal data, the lawful grounds for processing, and data subjects' rights and how those rights can be exercised and enforced.

Because the GDPR requires that notice be given to data subjects about specific processing activities and the notices must include things such as the purpose and lawful grounds for processing, it is difficult to bundle all of a controller's processing activities in the same policy. For this reason, controllers may need to provide separate notices for different processing activities, such as submitting admission forms, registering for conferences, registering for online courses, learning analytics, and so forth. Different schools and departments may also wish to provide their own notices. Nonetheless, higher-education institutions and other relevant organizations may also wish to provide one general privacy policy that states their underlying principles regarding personal data and their general approach to data privacy.

The GDPR does not require a specific method of communicating this information; it requires only that the information be provided to data subjects either at the time when their personal data is collected or, at the latest, within one month of obtaining the personal data when it is collected from other sources. In the latter case, if the personal data is collected from other sources in order to directly communicate with the data subject, the information must be provided, at the

latest, at the time of the first such communication. For example, if a university purchases names in order to send admissions brochures, the college must provide notice, either in the brochure or in a separate attachment, of processing activities.

Institutions should also provide notice if the university's website places cookies when visitors access it from Europe, as required by the ePrivacy Directive (Directive 2002/58/EC). Before obtaining consent for placing the cookies, the institution must provide information about the purposes and duration of the cookies and whether the information they access is shared with third parties. Visitors should be given the opportunity to actively give consent and to refuse cookies that are not necessary for the functioning of the website. In its recent judgment in the *Planet49* case, the Court of Justice of the EU found that pre-ticked boxes indicating consent are not lawful.[16]

For further guidance, see the official EDPB 2018 guidelines on transparency under the GDPR.[17]

## STEP 9: Identify All of the Organization's Data Processors, and Establish Controller-Processor Agreements With Them.

As noted at the beginning of this guide, the GDPR considers **processing** to be anything that can be done to personal data. The GDPR's legal definition of processing is "any operation or set of operations" performed on personal data, "whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4.2). This means that processing includes activities such as making personal data (such as an image of a person or an email address) available on a website, storing information, receiving information through online forms, keeping information or student records in paper files, displaying information on a smart board, and so forth.

The **controller** is the entity that alone or jointly with others establishes the means and purposes of processing. A controller can be an individual (natural person) or an organization (legal person). Most of the GDPR's statutory obligations are directed at controllers. Controllers are the ones responsible for ensuring that the processing of personal data complies with all of the regulation's data protection principles. In addition, controllers must perform due diligence when hiring vendors (processors) to process personal data on their behalf.
For example, a university uses an online form to

collect and analyze information about candidates' backgrounds, for undergraduate admissions. This activity involves the processing of personal data; the purpose of the processing is undergraduate admissions, and receiving applications via an online interface through a website is the means of this processing. The university establishes the purposes and means; therefore the university is the controller of this processing activity. If the admissions process is organized as part of a joint degree offered by two universities, then the two universities are joint controllers of this processing. To the extent that the processing falls under the GDPR, the two universities will have to enter a joint controllership agreement as required by Article 26 of the GDPR.

A **processor** is the entity that processes personal data on behalf of a controller. The processor is obliged to process personal data only on instructions from the controller. If the processor uses personal data received from the controller or directly collected by the processor for any purpose other than the one(s) for which it was mandated, or if it processes the data in any way outside the instructions received, then it becomes controller for that purpose(s) and will have to comply with all GDPR obligations for controllers.

For example, a university decides to use a service provider for online applications to its undergraduate program. In GDPR terms, the service provider is a processor and the university is a controller. If a university uses an online payment system to receive donations from alumni, the university is the controller and the online payment system is the processor. In both cases, Article 28 requires the two entities to enter a controller-processor agreement in which the controller details instructions for the processor, in order to process the personal data that falls under the GDPR.

Another common example of a data processor is a vendor that provides cloud storage services to a school or edtech app. The school or app provider collects and uses students' data for their own purposes, which makes them data controllers. These data controllers may hire a cloud provider to store the data. The cloud provider is the processor and must process the students' personal data solely for the purposes set out by the controllers and may not use it in any way other than what the controller authorized.

Depending on specific arrangements between schools and edtech apps, edtech apps may often be considered processors whenever they process personal data for the purposes established by a school, as in the first example of a processor noted above. In this case, a cloud services provider working in conjunction with the edtech app processor would be considered a sub-processor.

## STEP 10: Implement Technical and Organizational Data Security Measures.

The GDPR requires controllers to conduct a data protection impact assessment (DPIA) for certain high-risk activities (see Article 35 for details and criteria). Data protection impact assessments are in-depth analyses of potentially high-risk processing activities (conducted prior to the processing) to assess the likelihood and severity of the risk. These assessments need to consider the nature, scope, context, and purposes of the processing, and the sources of the risk. The assessment should also include the measures, safeguards, and mechanisms envisaged for mitigating the risks identified, to ensure the protection of personal data and demonstrate compliance with the GDPR (Recital 90).

Institutions need to conduct a DPIA only for processing activities "likely to result in a high risk," and the GDPR identifies some of the categories that meet this description. These include systematic and extensive evaluation of personal aspects of natural persons that is based on automated processing and that may have legal or significant effects on the data subject; large-scale processing of special categories of data; or large-scale systematic monitoring of a publicly accessible area.

For example, the CCTV monitoring of a campus in the EU falls under this description, as do learning analytics applications that may result in decisions that have significant effects on students. According to the GDPR, when a DPIA indicates that processing operations pose a high risk that the controller cannot mitigate by appropriate measures in terms of available technology and costs, the institution must consult the supervisory authority prior to the processing (Article 36, Recital 84—the "prior consultation" obligation).

The EDPB has published guidelines[18] on data protection impact assessments and information and guidelines[19] on processing personal data through video devices, such as CCTV cameras.

**Data protection by design**. The GDPR requires that controllers incorporate data protection rules in the design stage of and during processing (Article 25). The law requires that controllers implement both technical (e.g., encryption, pseudonymization) and organizational measures (e.g., managing access rights) in order to embed data protection principles in the processing. Such measures must be adopted by considering the state of the art; the cost of implementation; the nature, scope, context, and purposes of processing; and the likelihood and severity of risks that the processing may pose to individuals' rights.

The obvious context in which these obligations must be implemented is product development, but the GDPR language is broad enough to include any processing in which the establishment of the means of processing can absorb technical and organizational measures that ensure GDPR compliance. For example, an institution sets up an "active research projects" database to function as a one-stop shop for data on researchers, the names and purposes of all their projects, information about all the subjects of those projects, and the researchers' ongoing observations for each project. Such a database must include data protection principles from the outset.

For further information, see the guidance[20] on software development with data protection by design, published by the Norwegian Data Protection Authority, and the guidance on data protection by design[21] published by the EDPB.

**Data breaches**. The GDPR defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4.12).

In its guidelines on data-breach notifications, the EDPB defines specific types of data breaches:

- **Destruction** means that "the data no longer exists, or no longer exists in a form that is of any use to the controller";
- **Alteration** (or damage) means that "personal data has been altered, corrupted, or is no longer complete";
- **Loss** means that personal data "may still exist, but the controller has lost control or access to it, or no longer has it in its possession";
- **Unauthorized processing** "may include disclosure of personal data to (or access by) recipients who are not authorized to receive (or access) the data, or any other form of processing which violates the GDPR."[22]

Using well-known information security principles, the EDPB classifies personal data breaches as security incidents:

- **Confidentiality breaches** involve an "unauthorized or accidental disclosure of, or access to, personal data";
- **Integrity breaches** involve an "unauthorized or accidental alteration of personal data";
- **Availability breaches** involve an "accidental or unauthorized loss of access to, or destruction of, personal data."

Examples of personal data breaches include the following scenarios:

- A laptop containing copies of all admissions applications is stolen;
- The only copy of a set of personal data, such as evaluations of students, becomes encrypted by ransomware;
- The decryption key for encrypted data concerning students in a research project is lost, and the controller cannot restore access to the data, for example from a backup; Critical medical data about patients is unavailable, even temporarily, in the context of the operations of a hospital.

The GDPR requires that both controllers and processors implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The French Supervisory Authority, the Commission Nationale de L'informatique et des Libertés, has published a detailed guide[23] for ensuring the security of personal data under the GDPR.

For findings specific to higher education, see the UK's ICO 2019 report, "Findings from ICO information risk reviews of information security in the higher education sector."[24]

**Data-breach notifications**. Controllers are not required to notify supervisory authorities of a data breach unless the breach is likely to result in a risk to the rights and freedoms of natural persons. When controllers make such notification, they must do so within 72 hours after having become aware of the breach. Late notifications require an explanation for the delay.

Controllers also must notify data subjects of breaches "that may result in a high risk" to their rights and freedoms. The threshold for notifying data subjects is higher than that for notifying supervisory authorities. Data subjects need to be notified when the breach may lead to physical, material, or nonmaterial damage to them. Examples of such damage include discrimination, identity theft or fraud, financial loss, and damage to reputation. The GDPR considers these damages more likely to occur when the breach involves categories of data such as racial or ethnic origin, religious or philosophical beliefs, and health data.

When non-EU controllers are required to notify supervisory authorities of a breach, the controllers should notify the member state in which their legal representatives are based. Controllers who do not have legal representatives should notify the supervisory authority in the member state in which most of the affected data subjects are located.

Processors are required to notify controllers about all personal data breaches. The GDPR provides no threshold for notification of controllers; therefore, processors must provide notification for any incidents that meet the criteria for a personal data breach. The controller must then assess whether notification of supervisory authorities and/or data subjects is necessary.

In most scenarios, higher-education institutions are likely to be controllers. When they rely on processors, they need to include language in their controller-processor agreements that stipulates processors' obligation to notify controllers of any personal data breach. Nonetheless, even if such clauses are not included in the agreements, a processor is still required to notify a controller of any breaches that affect the personal data it processes on behalf of the controller.

**Sanctions for Noncompliance With the GDPR.** There are various sanctions for not complying with the GDPR, including administrative fines, penalties, and orders to suppress processing. Supervisory authorities have been tasked with the enforcement of the GDPR. Data subjects also have a direct cause of action for any breach of the regulation as well as the ability to be represented by an NGO in judicial or administrative proceedings in some EU member states.

Orders that may affect data flows. Supervisory authorities have specific powers granted directly by the GDPR that may affect data flows from the EU, including (but not limited to) the following actions:

- They can impose a temporary or definitive limitation, including a ban on processing;
- They can order organizations to comply with data subjects' requests to exercise their rights granted by the GDPR;
- They can order the suspension of data flows to a recipient in a third county or to an international organization.

**Administrative fines**. Supervisory authorities can impose administrative fines of up to 10 million euros or 2 percent of an organization's global annual turnover in cases of noncompliance related to

- Data protection by design;
- Data security, including notices of data breaches;
- Controller-processor agreements;
- Appointing a legal representative in the EU;
- Maintaining records of processing activities;
- Conducting data protection impact assessments.

Fines can go up to 20 million euros or 4 percent of an organization's global annual turnover in cases of noncompliance related to

- The basic principles for processing under the GDPR (lawfulness, transparency, purpose limitation, etc.), including conditions for valid consent;
- Data subjects' rights (such as access, erasure, etc.);
- Transfers of personal data to a recipient in a third country;
- An order issued by a supervisory authority to limit or ban processing, including suspension of data flows.

Individual cause of action. The GDPR provides for individual cause of action for data subjects who consider their rights to have been infringed due to noncompliance with the GDPR. Any person who has suffered either material or nonmaterial damage from a violation of the GDPR has the right to receive compensation from the controller or the processor for the damage suffered.

If a non-EU controller or processor violates one of the obligations outlined in the GDPR, enforcement of administrative fines is not straightforward, but given the broad powers of supervisory authorities, noncompliant organizations based outside the EU may, for example, see all data flows from the EU stopped (e.g., an internet service provider may be ordered to block all traffic attempts to a web page where people register for online courses). The law requires controllers and processors based outside the EU to appoint a legal representative in the EU, and one of the representative's roles is to be a contact point who ensures enforcement. Organizations that are found to be non-compliant and are issued fines, especially if they refuse to pay the fines, may also incur reputational damage.

# ENDNOTES


1 EUR-Lex, 2016, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," http://data.europa.eu/eli/reg/2016/679/oj.

2 Court of Justice of the European Union (CJEU), 2017, Case C-434/16 Nowak, December 20, para. 34.

3 European Data Protection Board, 2019, "Guidelines 3/2018 on the Territorial Scope of the GDPR," https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

4 Information Commissioner's Office, n.d., "Electronic mail marketing," https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/.

5 European Data Protection Board, 2018, "Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)," https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

6 Information Commissioner's Office, n.d., "Electronic mail marketing," https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/.

7 Ireland Data Protection Commission, 2019, "Guidance: A Practical Guide to Data Controller to Data Processor Contracts Under GDPR," https://www.dataprotection.ie/sites/default/files/uploads/2019-04/Guidance-for-Data-Processing-Contracts-GDPR.pdf.

8 See the EDPS's position paper, 2014, "The transfer of personal data to third countries and international organisations by EU institutions and bodies," https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf.

9 European Data Protection Board, 2018, "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679," https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

10 European Data Protection Board, 2018, "Guidelines on Consent under Regulation 2016/679 (wp259rev.01)," https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

11 European Data Protection Board, 2019, "Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects," https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

12 Hunton Andrews Kurth Privacy Blog, 2014, "Article 29 Working Party Issues Guidance on the 'Legitimate Interests' Ground in the EU Data Protection Directive," April 17, https://www.huntonprivacyblog.com/2014/04/17/article-29-working-party-issues-guidance-legitimate-interests-ground-eu-data-protection-directive/.

13 Future of Privacy Forum and Nymity, n.d., "Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases," https://fpf.org/wp-content/uploads/2018/04/20180413-Legitimate-Interest_FPF_Nymity-2018.pdf.

14 CJEU, 2017, "Judgment of the Court (Second Chamber) C-434/16 Nowak," December 20, http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=338232. For a summary of the guidance, see pdpEcho, 2017, "Exam scripts are partly personal data and other practical findings of the CJEU in Nowak," December 31, https://pdpecho.com/2017/12/31/exam-scripts-are-partly-personal-data-and-other-practical-findings-of-the-cjeu-in-nowak/.

15 For further details, see European Data Protection Supervisor, 2017, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit," https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

16 CJEU, 2019, "Judgment of the Court (Grant Chamber) C-673/17 Planet49," October 1, http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1447493.

17 European Data Protection Board, 2018, "Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)," August 22, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

18 European Data Protection Board, 2017, "Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)," October 10, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

19 European Data Protection Board, 2019, "Guidelines 3/2019 on processing of personal data through video devices," https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf.

20 Datatilsynet, n.d., "Software development with Data Protection by Design and by Default," https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/.

21 European Data Protection Board, 2019, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default," https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

22 European Data Protection Board, 2018, "Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)," https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Subsequent quotations in this section also derive from this document.

23 Commission Nationale Informatique & Libertés, 2018, "Security of Personal Data," https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.

24 Information Commissioner's Office, n.d., "Findings from ICO information risk reviews of information security in the higher education sector April 2017 to March 2018," https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2614196/20190124-information-risk-review-report-higher-education-sectorpdf.pdf.

1400 Eye Street NW, Suite 450 | Washington, DC 20005 | FPF.org

FUTURE OF PRIVACY FORUM