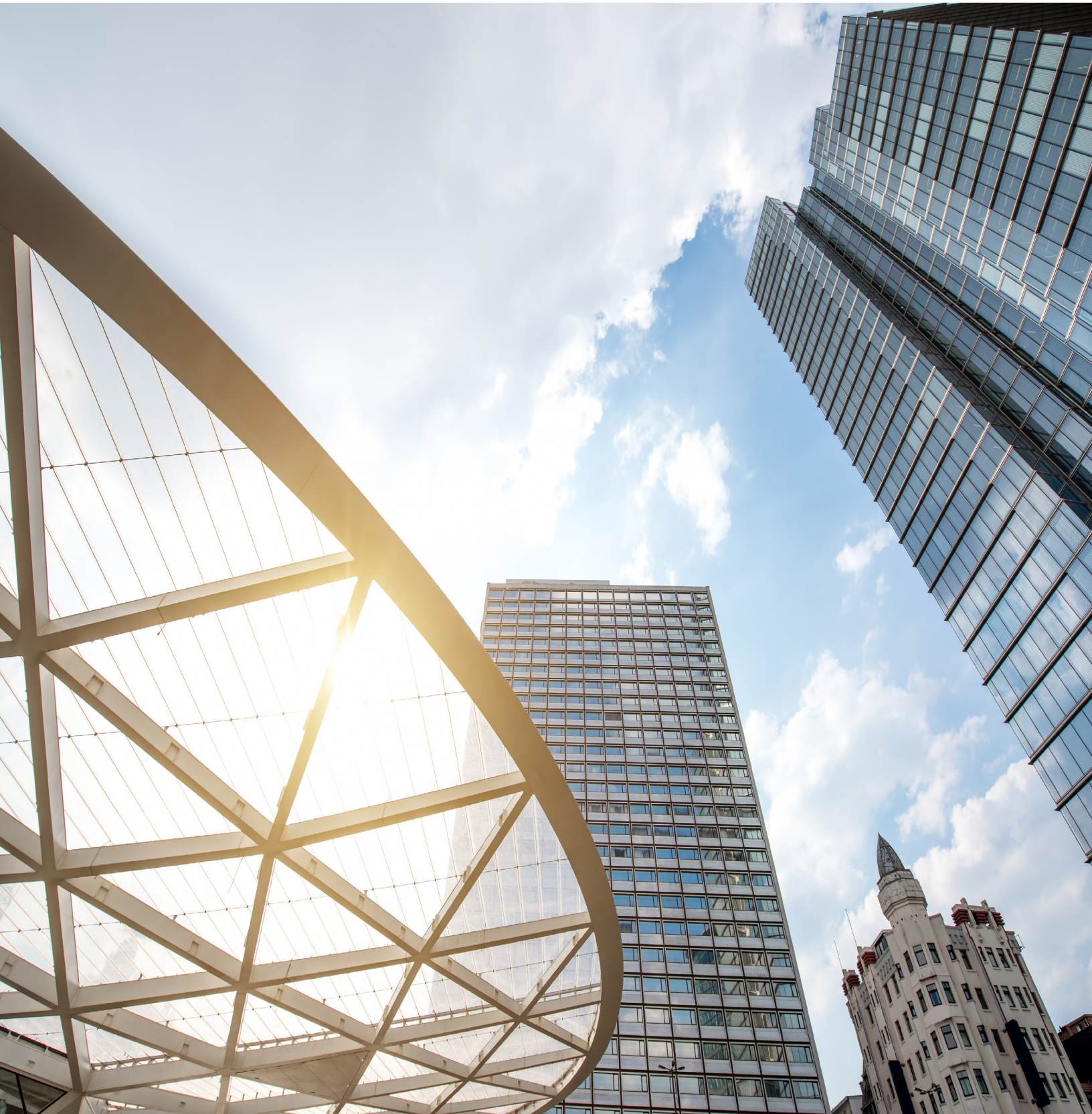
Implication of the General Data Protection Regulation

March 2018

AN INTERASSOCIATIONAL GUIDE
DISCUSSION DRAFT



Contributors

Mary Chapin
Vice President & Chief Legal Officer
National Student Clearinghouse

Joanna Grama
Director of Cybersecurity and IT GRC Programs
EDUCAUSE

Caroline Donovan White
Senior Director, Education Abroad Services
NAFSA: Association of International Educators

Tracy Locklin
Associate General Counsel
National Student Clearinghouse

Brian Flahaven
Senior Director, Advocacy
Council for Advancement and Support of Education (CASE)

Mark McConahay
Vice Provost and Registrar
Indiana University - Bloomington

Julia Funaki
Associate Director, International
American Association of Collegiate Registrars and Admissions Officers (AACRAO)

Joann Ng Hartmann
Senior Director for International Enrollment Management-International Student and Scholar Services
NAFSA: Association of International Educators

The Charge of the Working Group

The charge of the working group was to raise awareness, to inform and explain to our association members the European Union General Data Protection Regulation by providing background, an explanation of its' provisions, a foundation for conducting a risk assessment, and generally assist institutions in preparing their responses to the regulation. The group concentrated primarily on the administration of records associated with recruitment, enrollment, instruction and attainment of students. Though we are cognizant of other aspects of the higher education administration that require review, the working group's emphasis was on student administration.

Disclaimer

This document is intended to be a resource designed to assist the higher education community in preparing to comply with the EU General Data Protection Regulation, which goes into effect on May 25, 2018. The information, scenarios, and resources below are a compilation of materials developed by volunteers as part of an inter-associational effort. It is intended to provide general guidance only and is not intended, nor can it be relied upon, as legal advice.

An Inter-Association Collaborative Effort:

This document was the collaborative result of representatives from a wide array of professional higher education associations. The range of expertise and knowledge was invaluable in building a document in the short time period allotted. We collectively hope that our member institutions find the document of value.

The overall approach to the work was fairly simple. Once all agreed on the primary provisions of interest, the group agreed to develop information processing scenarios that would test the GDPR provisions in a higher educational context, discuss roles, considerations, and potential institutional responses to those provisions. The group was keenly aware that it could not offer legal advice for or on behalf of specific institutions, but did wish to provide sufficient information to provoke informed thought surrounding the issues. Thus, the document as presented includes:

Acknowledgements

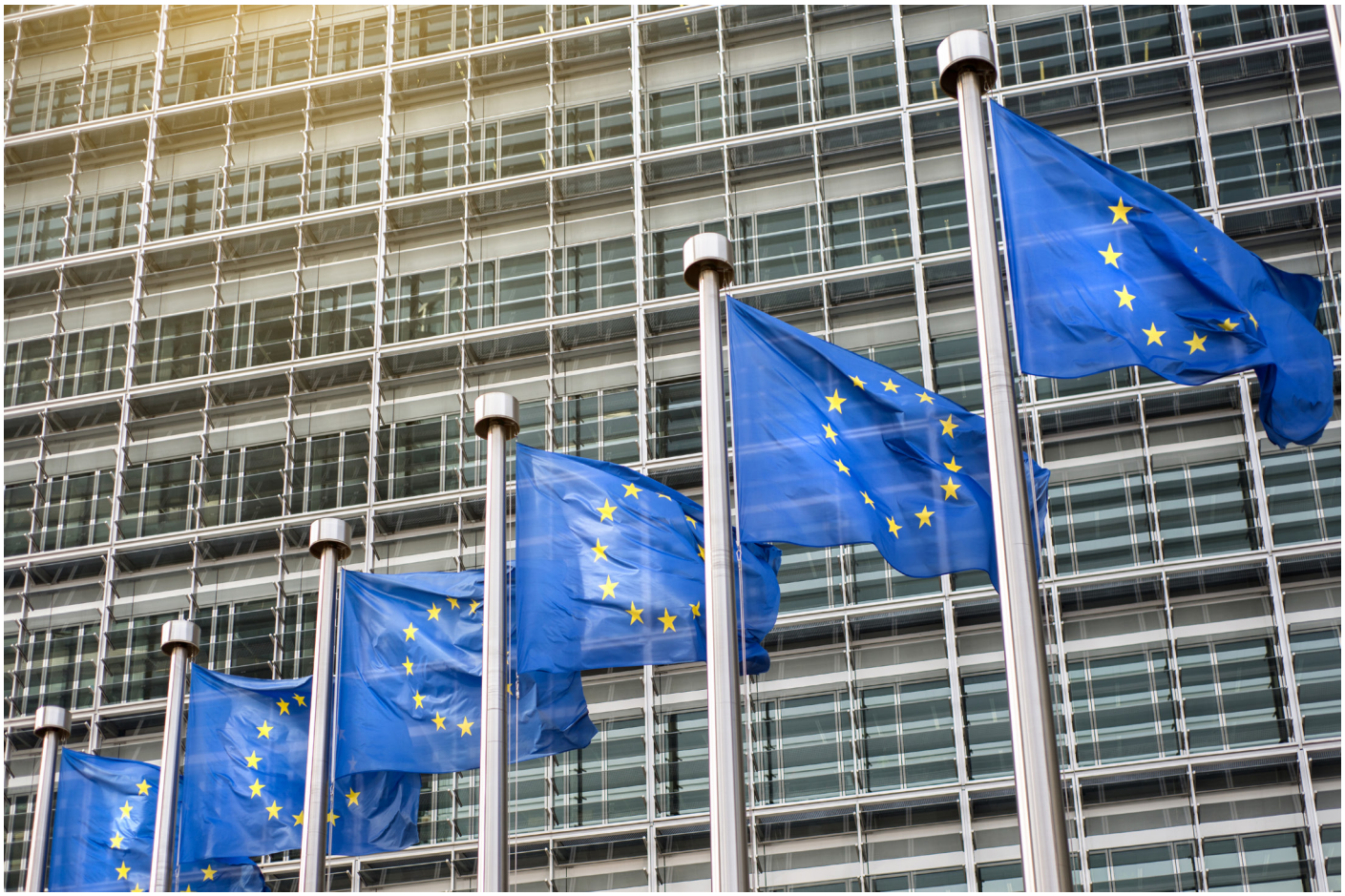
Bret Cohen, Partner, Hogan Lovells

Dr. David L. Di Maria, Associate Vice Provost for International Education
University of Maryland, Baltimore County

Anne Palmer, Director, Admissions Operations, Office of the Enrollment Management, Indiana University-Bloomington

Heidi Wachs, Special Counsel, Jenner & Block LLP

Background



In April 2016, the European Parliament, the Council of the European Union and the European Commission drafted a Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation or "GDPR"). This General Data Protection Regulation repealed and replaced Directive 95/46/EC (the "Directive").

As awareness of the GDPR grows and its implementation on May 25, 2018 nears, we have sensed increasing concern. GDPR provides an opportunity for higher education to engage in a process to identify and review our data flows, processing and management and update our policies and procedures. The information in this document and the other referenced resources help to explain the motivation and components of GDPR. Compliance and interpretation of the GDPR are legal issues. It is essential that you leave the legal issues to counsel.

What is the General Data Protection Regulation (GDPR)?

At its foundation the GDPR's purpose is to protect the data privacy of EU data subjects and deter data breaches of that data in an ever more globally digitized, data-driven reality. In addition, there was a strong desire to enable EU data subjects to control the disclosure and use of EU data subjects personal data. The European Union has done this before. The 1995 Directive outlined "the protection of individuals with regard to the processing of personal data and on the free movement of such data."[1] Although the key principles of data privacy still hold true from the Directive, this data-driven world is vastly different from the time in which the Directive of 1995 was established. The GDPR's regulatory policies close the gaps and bring into force the requirements for handling personal data in order to protect the fundamental right of individuals in the "Protection of Personal Data."[2]

1 EUR-Lex Access to European Union Law. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046. Accessed February 21, 2018.
2 EUR-Lex Access to European Union Law. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT. Accessed February 21, 2018.

GDPR offers key points of differences and changes to the Directive, the most notable include:

- **THE GDPR IS A REGULATION NOT A DIRECTIVE**
  - **"REGULATIONS ARE LEGAL ACTS DEFINED BY ARTICLE 288 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION (TFEU). THEY HAVE GENERAL APPLICATION, ARE BINDING IN THEIR ENTIRETY AND DIRECTLY APPLICABLE IN ALL EUROPEAN UNION COUNTRIES."**
  - **TERRITORIAL REACH (POSSIBLY WITH THE BIGGEST IMPACT ON OUR MEMBERSHIPS AND EDUCATION INSTITUTIONS AND ENTITIES)**
- **THE GDPR HAS PENALTIES**
  - **THIS IS A VERY SIGNIFICANT DIFFERENCE WHEN COMPARED TO THE 1995 DIRECTIVE AND THUS A MAJOR CATALYST FOR COMPLIANCE**
  - **GDPR'S TIERED APPROACH TO FINES WHICH CAN BE UP TO 2% OF GLOBAL TURNOVER FOR SOME INFRACTIONS AND A MAXIMUM OF 4% (OR UP TO 20 MILLION EUROS) FOR OTHER INFRACTIONS**
  - **GDPR'S BREACH NOTIFICATION REQUIREMENT INCREASES THE RISK OF ENFORCEMENT**

What is the General Data Protection Regulation (GDPR)? (continued)

Defining Personal Data

The GDPR and its articles refer to the processing of Personal Data, which for the purposes of the regulation, means any information relating to an identified or identifiable natural person ('data subject'). Thus, the EU definition of personal data is very broad. Whereas in the United States the processing of personal information is generally permitted and subject to a patchwork quilt of laws which define specific data elements as personal information (e.g., name in combination with SSN), which include sector based laws and regulations (e.g., Family Education Rights and Privacy Act [FERPA], Health Insurance Portability and Accountability Act [HIPAA], state data breach notification laws). In the EU, processing of personal data is generally prohibited unless certain requirements are satisfied.

A key point for U.S. readers is to understand that in the EU, "The protection of natural persons in relation to the processing of personal data is a fundamental right." This is quite different from U.S. based notions of personal privacy or the right against government intrusion into one's private dealings. Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union, provide that everyone has the right to the protection of personal data concerning him or her, or natural persons in the GDPR parlance.

Scope

In more specific terms, the Articles of the GDPR outline the requirements necessary for data handling, maintenance, and retention, collectively referred to as "processing." These requirements are what institutions need to consider in creating practices in order to comply with the GDPR. Quite simply, our systems need to adhere to data protection by design and default. (Article 25, GDPR) Some of the Requirements include:

Transparency (Article 12)
Individuals should be provided with notice on what personal data is being processed and the purposes for that processing

Consent (Article 7)
Should be clear and distinguishable

Breach Notification (Articles 33 and 34)
Mandatory and within 72 hours

Data Minimization (Article 5 and 25)
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Right to Access (Article 15)
Controller obliged to confirm and provide access to and copy of data - free of charge.

Right of Rectification (Article 16)
The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Right to be Forgotten (Right to Erasure) (Article 17)
There are conditions, but this does include right to erasure of data, halt in dissemination of data, and potentially halting third party processing of data.

Data Portability (Article 20)
Gives data subject right to obtain data in commonly used and machine readable format, and the right to transmit that data to another controller.

Privacy by Design (Article 25)
Meaning data protection at all stages and throughout a system. This may require a formal "certification" that processing platforms meet privacy requirements.

Data Protection Officers (Articles 37, 38, and 39)
Appointment of Data Protection Officers (DPOs) is intended to make adherence and compliance local and accountable.

GDPR outlines several items to ensure the DPO is equipped and supported in carrying out duties.

It is worth noting that many provisions above are similar (though not identical) to United States requirements on the use of data in certain instances and in certain sectors. For example, breach notification and data portability concepts are reflected in HIPAA. Concepts related to the right of rectification are reflected in FERPA. . What makes GDPR notable is that the provisions are comprehensive, universal, and not limited to certain data elements or industry sectors. Some provisions in the GDPR are somewhat novel. For instance, the GDPR "Right to be

Forgotten," which includes a data subject's right to object to or restrict processing of that person's data, is the provision that seems to provoke the most concern among higher education administrators.

The GDPR specifies two levels of responsibility for overall administration of data which is subject to GDPR provisions. In interpreting the GDPR and what steps are required to be compliant, it is important to understand which role your institution occupies and the roles of any processing partners. It should be noted that the role may vary based upon the nature of the processing and/or information which is being recorded, processed or disclosed. The roles as defined by the GDPR in Chapter 4 are:

Controller: the natural person or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data (Articles 24-43, of particular note - Articles 24-27)

Processor: a natural person or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Articles 24-43, of particular note - Articles 27-31)

For example, Institution A is a controller when it decides that it needs to collect certain types of data for admissions purposes through its use of cloud-based XYZ tool. Vendor B, the provider of XYZ tool, is a processor for Institution A during the admissions process.

Lawful Processing of Personal Information (Articles 5, 6)

Per the GDPR, an agency or institution should have a "legal basis" in order to process personal information of any European Union data subject. GDPR specifies two provisions in which personal data may be processed:

When necessary (Article 6)

To perform, or enter into, a contract with a data subject
To comply with a legal obligation
To protect vital interests of a data subject or another person
For the performance of a task carried out in the public interest
For legitimate interests pursued by the controller (can include first-party marketing!) or third party, except when such interests are overridden by the interests or rights of the data subject

With Consent (Article 6, Recitals 32, 40 and 43)

Must be freely given, specific, informed and unambiguous consent given by the data subject either by statement or clear affirmative action, which signifies agreement to the data subject's personal data being processed

It is important to understand the institutional legal basis for processing personal information with respect to these two provisions. In general, institutions may find it preferable to be able to specify when data processing is necessary (under the conditions outlined above), rather than relying upon receiving specific consent for

processing data. This is because the parameters for what constitutes successful consent to processing are so detailed. In U.S. higher education, our typical contract (in general) with students is, in exchange for the payment of tuition, to provide academic instruction and assessment within a defined curriculum and to support the success of the student within that curriculum. Presumably, the student would agree to enroll in the curriculum after notification and of the required processing to support it. One interpretation of this agreement could be that activities and processes directly supporting academic instruction of students could be performed per the GDPR as a necessary condition for fulfilling the institutional agreement with the student. Other activities and processes, not directly related to the academic mission, may require (specific) consent of the student before proceeding.

Motivation for Compliance

The GDPR is an opportunity. While it may not be your first thought, GDPR provides an opportunity for your institution to demonstrate its commitment to data privacy and protection. The penalties/fines might be the initial incentive to comply, but your protecting your institutional reputation may be the most compelling reason to pursue compliance. This is particularly true if you wish to recruit and serve students, faculty, or staff from the European Union. Your institution may not have a competitive advantage when compared to other institutions if you cannot demonstrate the basic privacy guarantees that students, faculty, or staff from the European Union expect. Were an institution not to comply, there would be financial repercussions, but perhaps even more, non-compliance would damage and potentially destroy their reputation.

Compliance with the GDPR can be a marketing opportunity for an education entity. Similar to an institution or association that highlights their environmental commitment and the image that conveys, compliance with the GDPR conveys to those encountering your institution that you care about protecting their data. GDPR compliance can be stated up front. It gives a sense of security to a data subject and a sense of pride to the controller or processor.

Risk Assessment and First Steps

Risk Assessment and First Steps

Who needs to be involved?

As we consider how to begin to review and evaluate our data processing and management, one possible approach is to create a GDPR Working Group to review GDPR's provisions and to develop an institution's overall compliance plan. You may want to consider members from the following areas:

GDPR Working Group
-University Counsel
-Information Security Officer/Unit
-Information Technology
-Representatives/stakeholders from functional units that process any kind of personal information. Examples of potential stakeholders may include Admissions, Financial Aid, Human Resources, Institutional Advancement, Education Abroad, International Programs, Online Education, and Athletics.
-Others specific to your institution

What does the Working Group Need to Consider?

The Working Group's charge is to investigate the provisions of the GDPR within the institution's context. A list of considerations could include:

- Identification of all populations affected
- Identification of functional-business units/areas affected
- Identification of existing policy germane to GDPR (e.g., FERPA, State Privacy regulations, Institutional policies, etc.)
- Examination of business processes/scenarios to identify
  - Where personal data is collected
  - Data pathways
  - Data repositories
  - Partner institutions, agencies, vendors involved with processing/storing/maintaining affected information
  - Impact of the GDPR on these processes
  - Scale of impact
  - Risk assessment
- Recommend practices/strategies to comply with the GDPR
- Identification of implementation costs and strategies

Sample Guiding Questions

A set of ample guiding questions to ask as part of this review is provided here and a preparation checklist can be found here: Preparing for the General Data Protection Regulation (12 Steps to Take Now) – Information Commissioner's Office (Disclaimer - Does not constitute legal advice).

Recurring Considerations for Responding to the GDPR Provisions

Territoriality

Determine if the provisions of the GDPR apply to your students and institution. It is imperative that institutions consult with legal counsel to understand this issue.

Careful consideration of Lawful/legal Basis for data processing

Identify data and processes that may be subject to the GDPR provisions and follow their life cycles and chain of custody.

It is very important to understand and define/describe the suite of services the institution is providing to students as they enroll at an institution, personal data that is collected, the direct processes that support them and what may be construed as in the best interest of the parties under Article 13. These considerations will enable the institution to set the boundaries on the fundamental components of their services and interpret the GDPR appropriately for their institutional context. This grounding also provides the foundation for clear and understandable notification to the student regarding the services and processes to support them. It will also enable the institution to identify processes or practices where student consent may be required.

Categorize GDPR Roles

Identify all third party organizations and/or service providers that operate or process information that may be subject to the GDPR provisions. Identify, in each instance, the role of your institution and/or a third party provider and the responsibilities associated with each.

Identify Processing Partners

For each partner determine their GDPR roles, your relationship with the partner, and what steps you need to pursue to insure the institution and your processing partners are compliant with GDPR provisions.

Recurring Considerations for Responding to the GDPR Provisions (continued)

Identify students who are subject to the GDPR and record it on the student record

Identify the students subject to the GDPR provisions unless the institution decides to treat all students as if they were subject to the GDPR.

Breach Notification (Articles 33 and 34, Recitals 85, 86, 87, and 88)

Clarify protocol at your institution for any breaches in security. The GDPR has provisions for mandatory reporting within 72 hourswhere student consent may be required.

The range of institutions represented by the member institutions of this inter-associational work group is very large and thus there are many data processes to be examined and reviewed for GDPR compliance. One methodology for attempting to measure impact of the GDPR at your institution is to identify primary data scenarios and apply the GDPR to the known process.

Methodology

Assessing and aggregating data processing scenarios should provide a solid foundation for deducing a set of common strategies and actions for complying with the GDPR. The emphasis in this document will primarily address the aspects of student information processing. Below are the areas covered.

Sample Case Scenarios

Sample Case Scenarios

- **ADMISSIONS AND ADMISSIONS OPERATIONS (CLICK HERE)**
- **ENROLLMENT REPORTING, VERIFICATION, AND DATA ANALYTICS SERVICES FROM THE NATIONAL STUDENT CLEARINGHOUSE - NSC (CLICK HERE)**
- **STUDY/EDUCATION ABROAD (CLICK HERE)**
- **SCHEDULING, ENROLLMENT AND ADVISING (AND RIGHT TO BE FORGOTTEN) (CLICK HERE)**

In each of the cases below we are providing a Situation and Questions regarding the scenario. In several of the scenarios, this is followed by a list of considerations using the Territorial Scope (Territoriality) and Roles (Controller and Processor) of the GDPR to pose questions for review and examination. We hope that this methodology for consideration of the impact of the GDPR on your institution will aid you to identify primary data scenarios and determine how to ensure your institutional process(es) comply with the GDPR. Once you identify and define your own scenarios, each can be examined for relevance to the GDPR requirements. Below is a possible template for your use and that we have used to consider the scenarios outlined.

Territoriality

- Does the scenario include personal data of persons subject to the GDPR provisions - EU data subjects?

Role(s)

- What role does the institutional and/or processing partner assume in the scenario?
- What is the role of the 3rd party partner?
- What is the obligation of both controller and processor?

Institutional Responsibility

- Is the processor GDPR compliant?
- Are all required notices provided and consents obtained at the time personal data is first collected?
- Other?

Institutional Actions

- What actions do we need to define to comply with GDPR?
- Do we include operational process in legal basis notification to student?
- Are we providing all required notices and obtaining all necessary consents?
- Have we implemented operational processes to respond to data subject access requests?

Admissions and Admissions Operations

Case 1.1 (Name Buys – multiple vendors):

SITUATION

Admissions purchases names and contact information from an external vendor (i.e., College Board, ACT, other).
(1) The student has given permission to the vendor to share their information with colleges and universities for the purpose of receiving recruitment information.

(2) Admissions loads the information to Slate (CRM), and in some cases to SIS.

(3) All recruitment e-mails provide the opportunity for opt-out.

QUESTIONS

(1) Can we assume that a student non-response is equivalent to an opt-out?

(2) If we purchase the same student's name from a different vendor, do we need to send a new communication? Would the previous opt-out (if one was received continue to be considered valid?

(3) Is there an expiration on opt-outs?

(4) If practice is to continue to communicate to the student until they opt-out or age out, based on the GDPR do we need to change and communicate only if we have an affirmative response (which might negatively impact open rate)?

Case 1.2 (Test Score receipt - from testing agencies):

SITUATION

A student requests that the testing agency send official scores to institution. Nightly downloads bring these scores into SIS. (Same process for all campuses.)
(1) If the student has applied, test score results are considered as part of the review.

i. Transactional (business) messages related to the application do not provide the opportunity for opt-out.
ii. Student should cancel their application if no longer interested.

(2) If the student has not yet applied, an SIS prospect record is created. Test score data is also imported into CRM, and student becomes part of the recruitment communication stream. If student is already an SIS Prospect, test score data is appended to the record in SIS and brought in to CRM.

QUESTIONS

(1) All recruitment e-mails provide the opportunity for opt-out.

i. Is the "opt-out" option for recruitment emails sufficient to be compliant with GDPR?
ii. Does an opt-out require that we delete the student record?

Admissions and Admissions Operations (continued)

Case 1.3 (Prospect data from applications in progress from Common App)

SITUATION

A student begins their application on one of these third party platforms, and has selected institution as one of the schools for which they intend to submit an application.

(1) By selecting our campus, the student has given permission to the vendor to share their information with colleges and universities for the purpose of receiving recruitment information.

(2) Admissions loads the information to CRM and SIS.

(3) We use the student information to drive the recruitment communication stream, with special messages encouraging them to complete and submit their application.

(4) All recruitment e-mails provide the opportunity for opt-out.

QUESTIONS

(1) Is the opt-out option in the recruitment messages sufficient to be GDPR compliant?

(a) Does an opt-out require that we delete the student record?

(2) Does admissions office become the controller upon receipt?

(3) Do our application vendors need to identify EU students?

Disclaimer: This document is intended to be a resource designed to assist the higher education community in preparing to comply with the EU General Data Protection Regulation, which goes into effect on May 25, 2018. The considerations for scenarios 1.1, 1.2, and 1.3 below are intended to provide general guidance only in order to provoke institutional thinking. It is not intended, nor can it be relied upon, as legal advice.

CONSIDERATIONS

Territoriality

- Did institution receive contact information of EU data subjects?

Role(s)

- Is 3rd Party controller as information is transmitted to institution?
- Is Institution controller once information is recorded and is to be used for recruitment?
- Is 3rd Party CRM the processor acting on behalf of the institution?

Institutional Responsibility

- Has Institution assured 3rd party partner is operating GDPR certified platforms?
- Has Institution assured 3rd Party identifies students subject to GDPR?
- Has Institution assured contact provider has obtained permission of student to share the contact information with institution?
- Has Institution assured initial contact with student will include notification regarding nature of contact/processing, include an opt-out for the contact?
- Did this include ability to notify student of process and capture a consent?
- Would Institution honor "right to be forgotten" if requested?

Institutional Action

- Should the Institution record personal information of students who are GDPR governed?
- Should Institution include option to "opt-out" and honor requests? Can it be assumed that it does not mean deletion of all contacts? Or not?
- Should Institution publish and include link on notification of Personal Information retention policies?

Admissions and Admissions Operations (continued)

Case 1.4 (Prospect data from applications from locally hosted application)

SITUATION

(1) Student submits application for admission. Campus provides information regarding our use of the information (for use in admissions evaluation and recruitment).
(2) Student reads and agrees to information use agreement.
(3) Admissions loads the information to CRM and SIS.
(4) Student information is used to drive the recruitment communication stream, with special messages encouraging them to complete and submit their application.
(5) All recruitment e-mails provide the opportunity for opt-out.
(6) Admissions becomes the controller upon receipt.

QUESTIONS

(1) Is the opt-out option in the recruitment messages sufficient to be GDPR compliant?
(2) Does an opt-out require that we delete the student record?
(3) Do our application vendors need to identify EU students?

Disclaimer: This document is intended to be a resource designed to assist the higher education community in preparing to comply with the EU General Data Protection Regulation, which goes into effect on May 25, 2018. The considerations for scenario 1.4 below is intended to provide general guidance only in order to provoke institutional thinking. It is not intended, nor can it be relied upon, as legal advice.

CONSIDERATIONS

(Note - The primary difference in this scenario is the application is institutionally built and managed).

Territoriality

- Did institution collect contact information of EU citizens while in the EU?

Role(s)

- Is Institution a controller?
- Is CRM vendor processor acting on behalf of Institution (controller)?

Institutional Responsibility

- Should the Institution describe the services/processes to be rendered upon data subject entering information into application?
- CRM Vendor - Will the Institution insure that the vendor is compliant with the GDPR and has a contract compliant with GDPR provisions?

Institutional Action

- Should the Institution record students who are GDPR governed?
- Can the Institution send the first communication? Is the communication required to provide sufficient information in first contact to describe nature of further contact/processing?
- Should the communication include option to “opt-out” and honor requests? Can the Institution assume it does not mean deletion of all contacts?
- Will the Institution honor a “right to be forgotten” and/or request to cease processing (recruiting)?
- Will the Institution publish (and include link on notification) personal information retention policies? If so, where will this be published?

Admissions and Admissions Operations (continued)

Case 1.5 (Alignment with AACRAO records retention recommendations/best practices for prospects, applicants, admits - non-enrolled): system): and Coalition App):

SITUATION

(1) Suspects who never respond to Institutions' communications.
(2) Prospects who never apply.
(3) Applicants who are not admitted.
(4) Admits who do not enroll.
(5) Assuming compliance at all stages, campus performs standard record retention processes for all records above.

Disclaimer: This document is intended to be a resource designed to assist the higher education community in preparing to comply with the EU General Data Protection Regulation, which goes into effect on May 25, 2018. The considerations for scenario 1.5 below is intended to provide general guidance only in order to provoke institutional thinking. It is not intended, nor can it be relied upon, as legal advice.

CONSIDERATIONS

Territoriality

- Did Institution collect contact information of EU citizens while in the EU?

Role(s)

- Is Institution a controller?
- Is CRM vendor processor acting on behalf of Institution (controller)?

Institutional Responsibility

- Does the Institution describe the services/processes to be rendered upon data subject entering information into application?
- CRM Vendor - Will the Institution insure that the vendor is compliant under the GDPR and has a contract compliant with GDPR provisions?

Institutional Action

- Would the Institution honor a "right to be forgotten" and/or request to cease processing (recruiting)?

Enrollment Reporting, Verification, and Data Analytics Services from the National Student Clearinghouse - NSC

Case 2.1 (Enrollment Reporting Service):

SITUATION

NSC enters into a contract with individual institutions pursuant to which an institution reports its student enrollment information to NSC and, on the institution's behalf, NSC receives and responds to requests from the National Student Loan Data System (NSLDS), other lenders and servicers in the federal student loan programs, and private lenders seeking to verify the enrollment status of student loan recipients, for purposes of ensuring that such enrolled loan recipients have their loans placed in deferment while they are in school

Case 2.2 (Verification Services):

SITUATION

For NSC's Degree Verification Service, NSC enters into a contract with individual institutions pursuant to which an institution reports its student degree data to NSC and, on the institution's behalf, NSC receives and responds to requests to verify an individual's degree from authorized requestors such as employers and background screeners. For NSC's Enrollment Verification Service, NSC enters into a contract with individual institutions pursuant to which an institution reports its student enrollment information to NSC and, on the institution's behalf, NSC receives and responds to enrollment verification requests of entities offering a product or service to enrolled students who have applied for the product or service for which the student's enrollment status is required

Case 2.3 (Data Analytic Services from the NSC):

SITUATION

NSC enters into a contract with individual institutions pursuant to which an institution reports its student enrollment and degree data to NSC and, on the institution's behalf, discloses the information to other postsecondary institutions, high schools, school districts, state departments of education, and outreach organizations to enable those entities to understand student pathways.

Case 2.4 National Student Clearinghouse:

SITUATION

Most institutions that participate in the federal student loan program send NSC enrollment data on their students monthly, which NSC then report to lenders and the U.S. Department of Education so that students can receive in-school deferments on their federal student loans. Among these institutions reporting enrollment data to NSC, there are a few institutions located within the EU which enroll students using federal student loans to pay for their course of study at the EU institution. In those cases, NSC acts a data processor of the enrollment data on behalf of the data controller, the EU institution, by reporting the enrollment data to lenders and the U.S. Department of Education.

Enrollment Reporting, Verification, and Data Analytics Services from the National Student Clearinghouse - NSC (continued)

Disclaimer: This document is intended to be a resource designed to assist the higher education community in preparing to comply with the EU General Data Protection Regulation, which goes into effect on May 25, 2018. The considerations for scenarios 2.1, 2.2, 2.3, and 2.4 below are intended to provide general guidance only in order to provoke institutional thinking. It is not intended, nor can it be relied upon, as legal advice.

CONSIDERATIONS

Territoriality

- Did institution receive/send contact information of EU citizens?

Role(s)

- Institution is a **c**ontroller as information is transmitted to institution.

NSC is a **p**rocessor. As a processor, NSC should comply with any instructions an institution (as a controller) provides to NSC regarding how it would like NSC to treat the EU personal data submitted to NSC for its services. It is up to the school to identify to NSC which information belongs to an EU student subject to the GDPR, when it provides to NSC a request under EU law (e.g., an opt-out).

Institutional Responsibility

- Controllers must contractually obligate processors to adhere to certain standards under the GDPR (Article 28).
- Institution (controller) is responsible for adhering to data privacy principles including providing notice consistent with the requirements outlined in Article 13 of the GDPR to those individuals covered by the GDPR. Article 13 of the GDPR requires, among other things:
  - Description of the purposes of processing (so the services should be described, at least at a high level), and
  - Description of the entities or categories of entities to which it discloses personal data covered by the GDPR (so the name of the specific service provider need not be disclosed).
- Institution should identify to NSC which information belongs to an EU student subject to the GDPR, when it provides to NSC a request under EU law (e.g., an opt-out).

Institutional Action

- Institution should record students who are GDPR governed.
- Institution should identify subject to the GDPR and specify how it would like to treat the EU personal data submitted to NSC for its services. The school should identify which information belongs to an EU student subject to the GDPR when it provides to NSC a request under EU law (e.g., an opt-out).
- Institution could consider the work performed by the NSC as "necessary for the purposes of legitimate interests" and thus considered lawful processing. If using this rationale, student must be granted the option of opting out of the process.
- Institution could consider the processing "necessary for the performance of the contract" but the institution needs to provide rationale for the processing. Thus, an institution would need to conclude that the relationship with the student could not exist without the processing of the data at issue.

Study/Education Abroad

Case 3.1 (University X student attends a study abroad or internship

SITUATION

(1) US citizen student attends an EU school via a mutual agreement above. Student attends for a semester, pays fees at home institution, and receives financial assistance from home institution. Student completes work at EU campus, student academic data transmitted to University X, noted and articulated to University X equivalent work.

i. Student is enrolled at X.
ii. Enrollment and performance records are transferred to X with student permission.
iii. The EU institutional data is articulated to X equivalents. Only the X course equivalents are recorded on transcript for subsequent reporting and distribution.
iv. EU records maintained only as source documents.

Disclaimer: This document is intended to be a resource designed to assist the higher education community in preparing to comply with the EU General Data Protection Regulation, which goes into effect on May 25, 2018. The considerations for scenarios 3.1, below are intended to provide general guidance only in order to provoke institutional thinking. It is not intended, nor can it be relied upon, as legal advice.

CONSIDERATIONS

Territoriality

- Did institution receive/send contact information of EU citizens?

Role(s)

- Institution is Controller while student is receiving services from institution
- Partner/consortia office is Controller while attending other institution.

Institutional Responsibility

- Insure the partner institution is GDPR compliant.

Institutional Action

- Receive and articulate work from partner institution. Record articulated values for institution.
- Delete data received from EU institution OR publish information retention policy (life cycle) for information received from partner institution.

Comment: Rationale for considering students domestic (and not subject to the GDPR) might be a consideration in this scenario. Rationale for making such a declaration should be documented.

Scheduling, Enrollment and Advising

Case 4.1 (International Student and Scholar Services - Record keeping

SITUATION

Jose from Spain did not have a good semester as a J-1 exchange student at University X. After a year, he emails the ISSS office to request that his record be erased as his GDPR right to be "forgotten". As part of record keeping and compliance, ISSS reports required data to DHS's Student and Exchange Visitor Program (SEVP).

Case 4.2 (EU Student enrolled at X. Learning Management System is a cloud based service used to administer classes in which the student is enrolled):

SITUATION

Student enrollment information is automatically shared with others in the same class. Some other elements may also be shared with instructor and classmates (e.g., student photo). Student evaluations, grades, correspondence and other artifacts are stored within the site and can be traced to student. Student actions within the system are recorded. IU mines the actions of all students in order to perform studies to improve instructional delivery, pedagogy and class learning outcomes.

QUESTIONS

(1) Will "legal basis" provide for the use of an LMS with regard to course administration?
(2) Will" legal basis" provide for the transfer of data to and use the third party system? (If yes, any exceptions to this?)
(3) ay X use the LMS data to improve course delivery, curricula and pedagogy without the EU student consent (is this use within our legal basis)?
(4) May the student invoke the right to be forgotten on this data? If so, do we need to classify the data maintained to determine if it is integral to legal basis (e.g., quiz scores, class assignments, email collaboration, correspondence with instructor, etc.)?

Case 4.3 (EU Student enrolled at X. Advising and Student Success system collect data/ attributes from faculty and staff regarding student academic actions and status):

SITUATION

(1) Instructors and advisors can record comments, attributes or other notations relating to a student ability to perform academically. Examples include: Attendance (or lack thereof), performing well, student in need of counseling or tutoring, additional assistance (e.g., writing) and many more. These records, generally, are not maintained as part of the permanent academic record, but may be germane for internal academic status and review.

QUESTIONS

(1) Will legal basis cover all uses of the data/system with regard to support of student success?
(2) May the student invoke the right to be forgotten on this data?

Case 4.4 Right to be Forgotten:

SITUATION

(1) A student from EU country has been academically dismissed and is now asking to "be forgotten". Are we required to comply?!?
(2) We had a data breach in 2014, and a student recently contacted us and requested that he "be forgotten" in our system. Does this come under GDPR?
(3) We have a student who has a large debt with our institution, which we have attempted to collect. They are stating their right to be forgotten and that we are not permitted to pursue payment. This isn't covered by GDPR, is it!?!

Scheduling, Enrollment and Advising (continued)

(4) We have an admission application for someone who applied to our institution 8 years ago, and is coming back to reapply. Currently we have those records, but is that still permissible under GDPR?

Case 4.5 (Affiliated Foundation) :

SITUATION

EU student graduates from institution that has an affiliated development foundation (institutionally related foundation). Typically, student information is shared with the foundation upon graduation.
(1) EU student enrolls at institution, resides in US for 4+ years and earns degree.

QUESTIONS

(1) Is consent required (or may legitimate interest be used) prior to sharing the information? (Earned degrees are public information in the US, which regulations apply?)
(2) Does the Foundation become a controller of the EU DS information?
(3) If Domestic student moves to the EU, do our terms of engagement change (must we now record the student as an EU DS)?

Case 4.6 (Institutional Advancement) :

SITUATION

Institutional advancement offices (development, alumni relations, communications, marketing and advancement services) conduct a number of activities covered by GDPR. How can advancement offices ensure compliance with GDPR in following common activities? :
(1) A college or university development office sends out an annual fund e-mail to its alumni, including alumni who are EU citizens and/or are located in the EU.
(2) A college/university/independent school conducts wealth screening on high net worth alums/supporters who live in the EU.
(3) An institution wants to hold an alumni event in London and wants to send out e-invites to alums located in the UK.

CONSIDERATIONS

A key consideration for institutions is whether to use consent or legitimate interest as grounds to process donor data. Regardless of which approach is chosen, institutions must be able to clearly explain their legal basis for processing donor data.

Sample Questions

- **HOW AND WHERE IS DATA STORED?**
- **WHO HAS ACCESS?**
- **WHAT INFORMATION IS ASKED OF THE APPLICANT?**
- **WHAT IS SHARED WITH HOSTING PROFESSORS?**
- **WHAT DO I NEED TO DO TO ENSURE THAT I AM COMPLIANT IN PROCESSING THE DATA OF THE APPLICANT?**
- **ARE MY RESPONSIBILITIES DIFFERENT FOR AN ADMITTED VS. DENIED APPLICANT?**
- **MUST WE ASK USERS OF OUR WEBSITE TO AGREE TO OUR TERMS BEFORE THEY PROCEED? IS THIS SUFFICIENT FOR GDPR?**
- **IS A PRIVACY NOTICE REGARDING THE USE COOKIES SUFFICIENT FOR GDPR?**
- **IS THERE AN EXPIRATION ON OPT-OUTS?**
- **CAN WE CONTINUE OUR PRACTICE TO COMMUNICATE WITH A STUDENT UNTIL THEY OPT-OUT OR AGE OUT? DO WE NEED TO CHANGE AND CONTINUE TO COMMUNICATE ONLY IF WE HAVE AN AFFIRMATIVE RESPONSE?**
- **IF BOTH PARTIES HAVE CONTROL OVER THEIR OWN SYSTEM AND DATA, WHAT ARE THE IMPLICATIONS OF THE CONTROLLER VERSUS PROCESSOR ROLES? WHERE IS THE DIFFERENTIATION?**
- **HOW DOES GDPR IMPACT DATA SHARING BETWEEN CONTRACTUAL PARTNERS?**
- **WHAT IF A CONTRACTED THIRD-PARTY RECRUITS THROUGH A NETWORK OF SUB-AGENTS?**
- **HOW CAN INSTITUTIONAL ADVANCEMENT OFFICES ENSURE THAT THEY ARE COMPLYING WITH GDPR?**
- **DOES GDPR APPLY TO A FACULTY MEMBER WHO TAKES SABBATICAL IN EU?**

Sample Questions
(continued)

- **IF WE HAVE A BREACH ON FRIDAY, DO WE NEED TO NOTIFY THE ADMINISTRATION, ALL STUDENTS OR JUST THE AFFECTED STUDENT? HOW CAN WE BE COMPLIANT WITHOUT CREATING A CAMPUS-WIDE PANIC?**
- **IF AN EU STUDENT CONTACTS A UNIVERSITY AND REQUESTS HIS RECORDS BE EXPUNGED; ARE WE OBLIGATED TO TAKE ACTION IMMEDIATELY, OR MAY WE FALL BACK ON PUBLISHED DATA LIFECYCLE?**
- **WILL LEGAL BASIS COVER ALL USES WITH THE LEARNING MANAGEMENT SYSTEM (LMS) WITH REGARD TO COURSE ADMINISTRATION?**
- **IS A BLANKET NOTIFICATION AND CONSENT REQUIRED FOR AN INSTITUTION TO TRANSFER DATA AND USE THE THIRD-PARTY SYSTEM? IF YES, ANY EXCEPTIONS TO THIS?**
- **MAY AN INSTITUTION USE THESE DATA TO IMPROVE COURSE DELIVERY, CURRICULA AND PEDAGOGY WITHOUT THE EU STUDENT CONSENT (IS THIS USE WITHIN OUR LEGAL BASIS)?**

Resources

AACRAO
Trending Topic Page

CASE
Currents article on GDPR considerations for advancement offices
GDPR Resource page (CASE member login required)

EDUCAUSE
All EDUCAUSE GDPR resources and links to other helpful resources can be found here. (Keep scrolling on the page for all relevant resources)

General Data Protection Regulation (GDPR) – Text and Recitals