GDPR & Higher Education Privacy Standards: A Global Perspective

Chair: Ricardo Torres, President & CEO
National Student Clearinghouse

Panelists:

Mary Chapin, Vice President & Chief Legal Officer National Student Clearinghouse, USA
Mehdi Gharsallah, Ministry of Higher Education, Research & Innovation, France
Melanie Gottlieb, Deputy Director, AACRAO, USA
Valere Meus, Coordinator, Erasmus Without Paper, Belgium
Audience Polling

Join at Slido.com

Event Code #5060
Global Data Protection

https://www.dlapiperdataprotection.com/

ONE DUPONT CIRCLE, NW SUITE 520 WASHINGTON DC 20036
Poll Question 1

Who is in attendance?

• University representative
• Governmental representative
• Non-Governmental Organizational representative
• Corporate entity representative
• Other
Poll Question 2

How knowledgeable are you about GDPR?

• Very Knowledgeable
• Somewhat knowledgeable
• Barely knowledgeable
• Not at all knowledgeable
GDPR Background:


• **Implementation** – May 25, 2018

• **Purpose** – to protect the data privacy of EU data subjects and deter data breaches of that data
Why do we care?

- Regulation
  - Legal act- binding in entirety and for all EU countries - Compliance
- Penalties
  - Significant difference over prior Fines
  - Breach notification requirements
- Security and Privacy are important
- Institutional Reputation
Definition of Personal Data

- Four Step Test*

  - Any information:
    - What qualifies as information
  - Relating to:
    - When does information relate to a person
  - An identified or identifiable:
    - What is identity?
    - When is someone identifiable?
  - Natural person:
    - What is a natural person?

- (Article 4, Recitals 26-27, 30)

*IAPP
Scope

- **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.
Levels of Responsibility (Role)

- **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)
Definition of Processing

Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure, destruction
Lawful Processing (Article 6; Recital 40)
(Lawful grounds; Legitimate Bases)

**Consent**
- Freely given
- Specific
- Informed
- Unambiguous
- Indication of wishes
Lawful Processing
(Lawful grounds; Legitimate Bases)

• When Necessary (Article 6; Recital 44)
  • To perform, or enter into, contract with data subject

• 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

• To comply with a legal obligation
• To protect vital interests of data subject or another person
• For the performance of a task carried out in public interest
Poll Question 3

Based on your current knowledge, do you consider your organization a:

- Processor
- Controller
- Both
- I am not sure
Poll Question 4:

For our EU colleagues:
From the standpoint of your organization, are you:

• Identifying only GDPR-subject records within current data structurers?
• Applying GDPR-compliance to all records?
• I am not sure
Poll Question 5:

For our NON-EU colleagues:
From the standpoint of your organization, are you:

• Identifying only GDPR-subject records within current data structurers?
• Applying GDPR-compliance to all records?
• I am not sure
GDN Principles & GDPR

PRINCIPLE 2: PRIVACY AND DATA PROTECTION

2.1. COLLECTION LIMITATION PRINCIPLE
2.2. DATA QUALITY PRINCIPLE.
2.3. PURPOSE SPECIFICATION PRINCIPLE
2.4. USE LIMITATION PRINCIPLE
2.5. SECURITY SAFEGUARDS PRINCIPLE
2.6. OPENNESS PRINCIPLE
2.7. INDIVIDUAL PARTICIPATION PRINCIPLE
2.8. ACCOUNTABILITY PRINCIPLE
Discussion

Questions?
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.
  - Define Legal Basis

- **Categorize GDPR Roles**
  - Identify all third party organizations and/or service providers.
  - Identify role of your institution and/or a third party provider and the responsibilities associated with each.

- **Identify Processing Partner**
  - 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.

- **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
Sample Questions from the US Institutional Perspective

- 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 of 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?
- 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

• General Data Protection Regulation (GDPR) – Text and Recitals - https://gdpr-info.eu/

• AACRAO Trending Topics: http://www.aacrao.org/resources/trending-topics/gdpr

• EDUCAUSE Library: https://library.educause.edu/topics/policy-and-law/eu-general-data-protection-regulation-gdpr

• The International Association of Privacy Professionals (IAPP): https://iapp.org

• Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf