Getting in the GDPR Groove: Planning and Executing Your Strategy

PRESENTED BY:
Heidi Wachs • Mark McConahay • Scott Schafer
A Brief Note from Heidi, Mark, & Scott:

• We are not giving legal advice;
• We are speaking in our individual capacities and not on behalf of any institution, organization, or company; and
• If you have specific questions you should consult the resources published by AACRAO, EDUCAUSE, NACUA, or your institutional counsel or compliance officer.
• This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution 4.0 International (CC BY 4.0), which grants usage to the general public, with appropriate credit to the author.
EU GDPR: AN OVERVIEW
What is the GDPR?

- General Data Protection Regulation ("GDPR") is a comprehensive data protection (data privacy) law for the European Union
  - Replaces the less expansive EU Data Protection Directive
Who’s the boss?

• Came into force on May 25, 2018, automatically and without further action by the legislatures of Member States
  – Local Data Protection Authorities (DPAs) will have authority to interpret the GDPR
  – New European Data Protection Board will provide guidance and adjudicate disputes between DPAs
  – Member States may establish more specific requirements (e.g., for employee data)
Does the GDPR apply?

• Applies to
  – Processing carried out in the EU
  – Organizations *outside* of the EU that offer goods and services to EU residents
  – Organizations *outside* of the EU that monitor the behavior of EU residents (i.e., track online behavior)
Data Controllers & Data Processors

• A “data controller” makes decisions about data processing

• A “data processor”
  – Data processors are required to maintain records of personal data and processing activities and will be subject to greater liability if responsible for a breach
  – Data controllers cannot push liability onto processors—must ensure contracts require processors to comply with GDPR
What data is covered? (1 of 2)

• Personal data
  – Any information “relating to an identified or identifiable natural person,” i.e., “one who can be identified, directly or indirectly”
  – The natural person is the “data subject”
  – Includes a name, an identification number, location data, and online identifiers, such as IP addresses, MAC addresses, etc.
  – Consider “all means reasonably likely to be used” to identify a person, when determining whether data is personal data

• But not anonymous data; relaxed standards for pseudonymized data
What data is covered? (2 of 2)

• Sensitive personal data (or “special category” personal data) – subject to heightened protection
  – Includes race or ethnic origin; political opinions or trade union membership; religious or philosophical beliefs; sexual orientation; and genetics, biometrics, health, or sex life
  – Processing requires
    • Explicit consent for a specified purpose, unless Member State passes law prohibiting use even with consent, or
    • One of several limited exceptions

• Personal data relating to criminal convictions or offenses
  – Processing must be specifically permitted by Member State law
What is data processing?

- GDPR defines “data processing” very broadly
- Processing essentially means use of individuals’ personal information and includes collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, or destroying personal data
Lawful Processing of Personal Data

• Must have a legal basis to process “personal data”
• Lawful conditions for processing
  – With consent of the data subject
  – To perform, or enter into, contract with 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
  – For legitimate interests pursued by the controller (can include first-party marketing!) or a third party, except when such interests are overridden by the interests or rights of the data subject
Basic Principles

• Transparency, lawfulness, and fairness
• Purpose Limitation
• Data minimization
• Accuracy
• Storage Limitation
• Security
• Accountability
Data Subject Rights

- GDPR creates new rights for individuals and strengthens some existing rights under the DPD
- Includes rights to
  - Be informed (notice)
  - Access personal data
  - Correct personal data
  - Data portability
  - Erase personal data
  - Restrict processing
  - Object to processing
  - Restrict automated decision making and profiling
- Different rights apply depending on the basis for processing
Accountability and Governance

• Must ensure—and be able to show—that you comply with the GDPR principles:
  – Controllers established outside of the EU must designate, in writing, a representative in the EU
  – Controllers that engage in “high risk” processing (large scale processing of “sensitive data” or profiling) must conduct privacy impact assessments
  – Certain controllers must appoint a Data Protection Officer (if core activity involves regular monitoring on a large scale or large scale processing of “sensitive data”)
  – Strict requirements for contracts with service providers
Data Breach Notification (1 of 2)

- “A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data…”
- Notify supervisory authority
  - If likely to result in “a risk” to individual rights and freedoms
  - Within 72 hours (unless law enforcement requests delay)
- Notify individuals
  - If likely to result in “high risk” to individual rights and freedoms
  - Without “undue delay”
  - Supervisory authority may instruct controller to notify individuals
Data Breach Notification (2 of 2)

• Information in breach notification
  – Nature of the records and approximate number and categories of individuals affected
  – Name and contact information for data protection officer or other contact point
  – Likely consequences of breach
  – Measures taken or to be taken to mitigate the breach

• Documentation by data controller
  – Record of facts related to the breach, its effects, and the remedial measures taken

• Significant fines for non-compliance
  – Fines of up to € 10,000,000 or 2% of annual global turnover, whichever is higher
Cross-Border Data Transfers

• Transfer of personal data outside the European Union includes access

• Personal data may be transferred out of the EU if an approved transfer mechanism is in place or one of a list of pre-approved derogations applies

• Derogations

• Penalties for non-compliance
  – Fine of up to 4% of annual global turnover
Enforcement

• DPAs are given extensive authority
  – Monitoring and enforcing compliance with the GDPR
  – Conducting investigations
    • Ordering companies to provide information
    • Conducting audits
  – Issuing warnings
  – Imposing fines
  – Banning processing and cross-border data transfers

• DPAs’ actions are subject to judicial review

• DPA from Member State where principal establishment of company is domiciled will be “lead” authority in cross-border cases
Remedies and Penalties

- Individuals have a right to
  - Lodge complaints with DPAs against controllers and processors for non-compliance with GDPR
  - Seek judicial remedies against controller or processor or judicial review of DPA decision
  - Compensation for damage resulting from non-compliance with GDPR from both controllers and processors

- DPAs may impose fines or other injunctive measures
- Fines are discretionary and must be imposed on case-by-case basis
- Two tiers of fines:
  - (1) Up to € 10 million, or 2% of annual global turnover, whichever is higher, and
  - (2) Up to € 20 million, or 4% of annual turnover, whichever is higher
Enforcement Actions

- UK ICO issued first formal enforcement action in July 2018:
  - Aggregate IQ Data Services – Canadian Data Analytics Firm
  - Used names & email addresses for data analytics for political purposes
- UK ICO Ruling:
  - “Processed personal data in a way that data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for processing”
- Enforcement action:
  - Cease processing any personal data of UK or EU citizens for data analytics, advertising, or political campaigning
  - Failure to comply with enforcement action would require up to 20 mil Euros or 4% total turnover
A Practitioner’s Perspective: An Overview of IU’s GDPR Strategy for Student Data from a University’s Registrar

Mark McConahay, Associate Vice Provost and Registrar, Indiana University, Bloomington
Agenda

• AACRAO Inter-associational Guide
  – Approach
  – Content
  – First Steps

• An Institution’s Evaluation Process
Implications of the GDPR: An Inter-Association Guide*

- The charge of the working group was to:
  - raise awareness,
  - to inform and explain
  - Provide foundation for conducting a risk assessment,
  - generally assist institutions in preparing their responses to the regulation.

*Participants from: AACRAO, Indiana University Bloomington, Council for Advancement and Support of Education (CASE), EDUCAUSE, National Student Clearinghouse, NAFSA: Association of International Educators, NACAC, NASPA
Our Approach

• Reach agreement on primary provisions
• Develop information processing scenarios
  – test the GDPR provisions in a higher educational context
• Include:
  – roles,
  – considerations, and
  – potential institutional responses to those provisions.
Content of the Guide

• Background
• Risk Assessment and First Steps
  – Guiding Questions
• Recurring Considerations for Responding to GDPR Provisions
• Sample Case Scenarios
  – Admissions and Admissions Operations
  – Enrollment Reporting, Verification, and Data Analytics Services from the National Student Clearinghouse
  – Study/Education Abroad
  – Scheduling, Enrollment and Advising (and Right to be Forgotten)
• Resources
Institutional First Steps

Form EU-GDPR Working Group
- University Counsel
- University Security Office
- University Information Technology Services
- University Data Administration Officials (Stewards)
- Functional unit representatives

Working Group Charge
- GDPR - context of your institution
  - Identify populations affected
  - Identify functional/business areas
  - Examine processes and scenarios to measure scope of impact
- Analyze/Identify common elements
- Recommend practices/strategies to comply with GDPR
- Identify implementation costs and strategies
Student Records and the EU GDPR

• Discussions regarding campus response to the GDPR
  – Led by University Counsel
  – IU Chief Privacy Officer
  – Operational/Functional Officers
    • e.g., Registrar, Office of Online Education, etc.

• Primary operational categories for Student Records:
  – Admissions and Recruitment
  – Enrolled Students
  – Post Enrollment
Admissions and Recruitment

Territoriality

- Campus scenario of potential data subjects for an academic year:
  - Undergraduate EU students/potential students
    - ~5,000 students in recruiting cycle
    - ~500+ applicants/~500 Admits
    - ~75 Enrollments/AY
- ~500 EU Enrolled Students
- ~120 Graduates/year
Admissions & Recruitment

Recommendations

Scenario
- ADMS Funnel:
  Is home address in the EU?
- How is data subject recruited to campus
  - Potential DS under GDPR provision
- Potential Students Rights
  - E.g., Request by DS to delete their data

Considerations
- Considered data subject under provisions of GDPR?
  - Goods/Services or Tracking?
- Can/should we record status?
  - Mechanism for flagging in SIS?
- Provide Privacy Notice?
  - When? How?
- Can we comply?
  - Process for deletion?
Admissions & Recruitment

Recommendations

• Scenario
  • Recruit GDPR Data subjects
  • Processors (process data on our behalf)
  • Class of 2018 recruitment nearly complete

• Recommendation
  • GDPR:
    – Include in privacy notice
    – Internally document our interpretation and operational practices
  • Obtain working agreements with processors (CRM)
  • Begin GDPR data practices with 2019 recruitment class
Enrolled Students

• Students residing in the US, enrolled in US
  – Considered subject to US privacy laws

• Online Participation Students
  – Residing in EU – data may need to be treated as subject to GDPR
  – Determine true number/scale of EU data subjects
    • If relatively small, manage manually
  – Notify processing partners if students treated as GDPR data subjects
  – Must notify students treated as GDPR data subjects
Post Enrollment

• Similar to enrolled students above, domestically enrolled students not subject to GDPR
  – Thus, initial processes and operations involving data/information transfer between Campus and affiliates (Alumni, etc.) should remain unchanged...

• Continuing analysis for those students returning to EU.
  – Additional goods/services/asks?
  – Client Mobility
  – Vendor Roles
Selected Resources

- **Implications of GDPR: Interassociation Guide** 05.15.2018

- **Helix Education** Published on Jun 3, 2018 (Mark McConahay with bowtie and sandals)

EU GDPR:
AN INSTITUTIONAL APPROACH

Scott D. Schafer
Chief University Privacy Officer and
Institutional Compliance Officer
University of Pennsylvania
What Do We Mean By Institutional Approach?

Who is Responsible for Overall Approach to GDPR?

• Identify Who “Owns” Responsibility for Coordinating Overall Strategy to GDPR
  • Compliance
  • Privacy
  • IT
  • Office of General Counsel
• Allows for a Risk-Based Approach
• Ensures Consistency and Avoids Conflicting Approaches to Compliance
• Ability to Assess GDPR Readiness and Compliance on an Institutional Level
What is Your Risk Profile?

Low Likelihood of Enforcement

➢ Not in EU
➢ Universities Not Likely Priority Targets
➢ BUT not Exempt
  o Individuals Could File Complaint
  o Data Breach Could Trigger Enforcement Action

High Impact in the Event of Enforcement Action

➢ Potential for High Fines
➢ Reputational Harm
What is Your Risk Profile?

GDPR Compliance

LIKELIHOOD

IMPACT
What University Activities Are Higher Risk?

- Study-Abroad Programs and Overseas Offices
- Executive Education and Distance Learning
- Admissions
- Registrar/Student Records
- Alumni Relations
- Employees Based in EU
- Research Centers
- Vendors
When Do I Need to Comply?

Effective Date: May 25, 2018

You Are Not Alone

April 2018 - Cloud Security Alliance Says 83% of Global Companies Not Ready for Europe's GDPR

May 2018 - Reuters: 17 out of 24 EU Regulators Not Ready

➢ Not passed the necessary enabling legislation
➢ Not funded for enforcement
How Do You Approach GDPR Compliance?

<table>
<thead>
<tr>
<th>BUILD</th>
<th>ASSESS</th>
<th>DESIGN</th>
<th>IMPLEMENT</th>
<th>COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Stakeholders</td>
<td>Identify GDPR Triggers</td>
<td>Processes for:</td>
<td>Identified Processes</td>
<td>Regularly Review Processing Activities</td>
</tr>
<tr>
<td>Allocate Resources</td>
<td>Conduct Gap Assessment</td>
<td>• Consent and Notice</td>
<td>Policies and Notices</td>
<td>Maintain Reporting that Demonstrates GDPR Compliance</td>
</tr>
<tr>
<td>Appoint DPO</td>
<td>Assess Risks vs. Level of Effort</td>
<td>• Data Subject Rights</td>
<td>• Privacy Impact Assessments</td>
<td>Schedule Periodic Audits</td>
</tr>
<tr>
<td>Define Program Mission &amp; Goals</td>
<td></td>
<td>• Data Transfer</td>
<td>• Physical, Technical and Administrative Safeguards</td>
<td></td>
</tr>
<tr>
<td>Create Awareness</td>
<td></td>
<td>• Legal Basis for Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Breach Notification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vendor Contracts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 2017
2. 2018
3. 2019
What Activities Should I Prioritize?

Taking a Risk-Based Approach

➢ Mapping Data with Key Stakeholders
➢ Updating Privacy Notices
➢ Documenting Processing Activities
➢ Obtaining Proper Consents If Necessary
➢ Implementing Processes to Honor Requests
➢ Reviewing Vendors and Data Transfer Mechanisms
➢ Incident Response
What are Some Complex Issues or Difficult Questions?

• Do I need a DPO?
• How Do I Handle a Data Subject Request?
  ➢ Verification
  ➢ Response
• Thinking About Data – Collection, Use, Disclosure
• Decentralization -- Owner of Data Platform May Not Know the Data, Use, or Disclosure
How Do I Data Map?

❑ What?
  What Information is involved?
  Is it personal or sensitive information?

❑ Why?
  Why is the data being collected?
  Is the purpose allowed? Did you provide notice or get consent?

❑ Who?
  Who is it being shared with? Third-party?
  Is this person authorized? Contract in place if third party?

❑ How?
  How is it being shared?
  Is it sufficiently secure?
GDPR: Privacy Trend or Anomaly??

June 28, 2018

California Consumer Privacy Act
Please take a moment to evaluate this session
There are two ways to access the session and presenter evaluations

1. In the online agenda, click on the “Evaluate Session” link

2. From the mobile app, click on the session you want from the schedule > then click the associated resources > and the evaluation will pop up in the list