How Does the General Data Protection Regulation Affect Colleges and Universities?

November 29, 2018

Sponsored by Cornerstone
Presenters

Joanna Grama, JD, CISSP, CRISC, CIPT
Senior Consultant, Former Director of Cybersecurity and IT GRC Programs at EDUCAUSE Vantage Technology Group

Scott Schafer
Chief University Privacy Officer and Institutional Compliance Officer University of Pennsylvania
ABOUT US

• Scott Schafer
  • Chief University Privacy Officer and Institutional Compliance Officer
  • University of Pennsylvania

• Joanna Grama
  • Senior Consultant
  • Vantage Technology Consulting Group
AGENDA

OVERVIEW OF GDPR AND ITS REQUIREMENTS

LESSONS LEARNED IN THE PAST SIX MONTHS

THINKING STRATEGICALLY ABOUT GDPR
OVERVIEW OF GDPR AND ITS REQUIREMENTS
POLL QUESTION

• Have you ever heard of GDPR?
  • Yes
  • No
  • Maybe
  • I think the IT people talked about it once
GDPR

What is GDPR?
  • EU General Data Protection Regulation

When Does It Apply To U.S. Institutions?
  • Physical Presence in EU
  • Offer Goods and Services Targeting EU Residents
  • Monitoring Behaviors of EU Residents
  • Includes Website Tracking/Analytics targeting EU residents

What Does it Apply To?
  • Personal Data
  • Broadly Defined
  • Data from which a living individual is identified or identifiable, whether directly or indirectly
KEY REQUIREMENTS

- Fair Processing Notices
- Honoring Data Subject Rights – 30 Days
- Document Legal Bases For Processing Data
- Privacy Impact Assessments for New Processes/Projects
- Determine Data Transfer Mechanism
- Data Breach Notification – 72 Hours
SPECIAL CATEGORIES OF DATA

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data used for the purpose of uniquely identifying a natural person
- Health Information
- Sexual orientation or data related to sexual behavior
- Criminal history
## RISK PROFILE

### Low Likelihood of Enforcement
- Not in EU
- Universities Not Likely Priority Targets
- BUT not Exempt
  - Individuals Could File A Complaint
  - Data Breach Could Trigger Enforcement Action

### High Impact in the Event of Enforcement Action
- 2% Global Turnover or €10M
  - Failure to notify of data breach
- 4% Global Turnover or €20M
  - Violation of Individual Rights
  - Reputational Harm
POLL QUESTION

• Which institutional activities may be impacted by GDPR? (choose all that apply)
  • Study-Abroad Programs
  • Admissions
  • Alumni Relations
  • Employment Recruiting
  • Research Centers
UNIVERSITY ACTIVITIES

• Study-Abroad Programs and Overseas Offices
• Distance Learning
• Admissions
• Registrar/Student Records
• Alumni Relations
• Employees Based in EU
• Research Centers
• Vendors
GDPR READINESS

• 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
REAL WORLD CHALLENGES

• **Thinking About Data** – Collection, Use, Disclosure

• **Decentralization** – Owner of a data platform may not know the data, uses, or disclosures

• **Uncertain Regulatory Guidance**
  • Still evolving guidance
  • We need to continue monitor
  • 6 months later still a lot of unknowns
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
MORE STATISTICS

- The first GDPR complaints were filed within an hour of the regulation coming into force.
- In the first month of enforcement, self-reported breaches in the UK increased by a factor of 5 over the previous month.
- Between May 25 and October 1, 2018, the CNIL received 742 notifications of personal data breaches that affected 33,727,384 individuals located in France or elsewhere.
POLL QUESTION

• Is the GDPR an anomaly or a trend?
  • Anomaly
  • Trend
  • The future is unclear
GDPR: PRIVACY TREND OR ANOMALY?

- California Consumer Privacy Act (June 28, 2018)
- EDUCAUSE 2019 Top 10 IT Issues
  - #3 is Privacy, likely due to GDPR influence
THINKING STRATEGICALLY ABOUT GDPR
WHAT DO WE MEAN BY INSTITUTIONAL APPROACH?

- Identify Who "Owns" Responsibility for Coordinating Overall GDPR Strategy
  - Compliance
  - Privacy
  - IT
  - 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
GDPR READINESS

Issues to Think Through:

• Taking a risk-based approach
• Mapping your data
• Updating privacy notices
• Documenting processing activities
• Obtaining proper consents for special categories of data
• Implementing processes to honor individual requests
• Reviewing vendors and data transfer mechanisms
• Incident response
POLL QUESTION

• Does your institution have a privacy policy?
  • Yes
  • No
  • I don't know
  • Privacy is dead.
IMPLEMENTATION APPROACH

Phase 1

BUILD
- Identify Stakeholders
- Allocate Resources
- Define Program Mission & Goals
- Create Awareness

Phase 2

ASSESS
- Map Data
- Identify GDPR Triggers
- Conduct Gap Assessment
- Assess Risks vs. Level of Effort

DESIGN
- Processes for:
  - Consent and Notice
  - Data Subject Rights
  - Data Transfer
  - Legal Basis for Processing
  - Data Breach Notification
  - Vendor Contracts

Phase 3

IMPLEMENT
- Identified Processes
- Policies and Notices
- Privacy Impact Assessments
- Physical, Technical and Administrative Safeguards

COMPLIANCE
- Regularly Review Processing Activities
- Maintain Reporting that Demonstrates GDPR Compliance
- Schedule Periodic Audits
THE “ASK”

Commitment of Resources
- Personnel from Key Stakeholders for Project Team

Participate in Assessment
- Map Data in Key Risk Areas
- Identify Gaps
- Determine Effort vs. Risk

Design and Implement Processes
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?

How?
- How is it being shared?
- Is it sufficiently secure?
POLL QUESTION

• Does your institution have a data map?
  • Yes
  • No
  • I don't know
  • Can I get it at AAA?
## Data Mapping Table Template

<table>
<thead>
<tr>
<th>Personal Data Type</th>
<th>Data Source</th>
<th>Is Privacy Notice provided?</th>
<th>What Do We Use The Data For?</th>
<th>Who Is The Data Used By?</th>
<th>Where Is Data Processed/ Stored?</th>
<th>Future Potential Users for Data?</th>
<th>Basis For Our Processing Under GDPR?</th>
<th>Are We A Data Processor Or Data Controller?</th>
<th>Retention Period</th>
<th>Special Categories Of Data – Yes/No?</th>
<th>Who Is The Data Processor?</th>
<th>Are They Internal Or External?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alumni name, address, demographic information, donor history, relatives</td>
<td>Data subject direct</td>
<td>Yes</td>
<td>Direct mailings</td>
<td>Gifts team</td>
<td>On our alumni database which is hosted in the cloud but specified as located in the EEA, namely Ireland</td>
<td>Inviting customers to events</td>
<td>Legitimate interests and also data subject has given consent</td>
<td>Data controller</td>
<td>2 years since last contact or removal of data</td>
<td>Yes – usual and administrative affiliation</td>
<td>Outsourced mailing provider</td>
<td>External</td>
</tr>
</tbody>
</table>
HAPPY READING


Q & A

Joanna Grama
Senior Consultant, Former Director of Cybersecurity and IT GRC Programs at EDUCAUSE
Vantage Technology Group
joanna.grama@vantagetcg.com

Scott Schafer
Chief University Privacy Officer and Institutional Compliance Officer
University of Pennsylvania
sschafer@upenn.edu
Thank You!

How Does the General Data Protection Regulation Affect Colleges and Universities?

November 29, 2018

Sponsored by Cornerstone