GDPR + 6 Months: What We Know Now, What We Wish We Had Known Then

EDUCAUSE Live! Webinar
November 19, 2018

Webinar Objectives

- Obtain a high-level understanding of the GDPR and its more significant requirements
- Learn from one large university's GDPR compliance journey and how its path may inform yours
- Get an update on significant actions or interpretations of GDPR since it went into effect in May 2018

Sol Bermann
Interim CISO and Privacy Officer
University of Michigan

David Grimm
Associate General Counsel
University of Michigan
Disclaimer

All materials have been prepared for general information purposes only. Given the changing nature of laws, rules and regulations, there may be omissions or inaccuracies in information contained in this presentation.

The information presented is not legal advice, should not be acted on as such, and is subject to change without notice.

Why GDPR: How did we get here?

European Socio-political History

Hitler’s Gestapo
Stalin’s NKVD
Honecker’s Stasi
Salazar’s PVDE
Franco’s Secret Police
**Why GDPR: How did we get here?**

European Politico-legal History

---

**1948: UN Declaration of Human Rights (Art. 12)**
- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

**1995: Directive 95/46/EC of the European Parliament** on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Art. 1, 1)
- In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

---

Meanwhile in the United States...

---

**HIPAA**
Health Insurance Portability and Accountability Act

**FERPA**
Family Educational Rights and Privacy Act

**COPPA**
Children’s Online Privacy Protection Act
Approach to Privacy

You CAN collect data, unless...

The law says you **can’t**

You CANNOT collect data, unless...

The law says you **can**

---

GDPR Basics

EU General Data Protection Regulation is a legally enforceable regulation passed to replace the EU Data Protection Directive.

Its goal is to harmonize the regulations and protections for individuals with respect to data processing and to safeguard the free flow of information between member states, and the world.

GDPR attempts to regulate data controllers and processors inside and outside of the EU.

GDPR became effective on May 25, 2018.
GDPR: PII and Then Some...

Typical Personally Identifiable Information

- Name and surname
- Home address
- Email address
- Identification card number
- Location data (e.g. the location data function on a mobile phone)
- Data held by a hospital or doctor that uniquely identifies a person
- SSN/Government identifier

But GDPR definition also includes:

- Internet Protocol (IP) address
- Cookie ID
- Advertising identifier of a phone
- Content of exam papers
- Any information relating to an identified or identifiable natural person

When GDPR Likely Applies in Academia

A cohort of non-EU students is participating in a semester-long study abroad in Italy, Belgium, and France.

Office of Development is engaged in a fundraising campaign and is collecting donor information from alumni residing in the EU.

A research consortium in the EU provides the university with the personal data of EU citizens for research analysis.
University of Michigan’s Approach

Review GDPR requirements and develop a risk-based compliance strategy and corresponding compliance program.

- **People**: engage the right stakeholders, document GDPR roles & responsibilities
- **Policy**: provide privacy statements and supporting templates & documentation
- **Process**: assess and address processes in support of compliance
- **Technology**: identify possible technical solutions enabling compliance
The U-M GDPR Project

Key Project Accomplishments

- Recommended appointment of Data Protection Officer (DPO)
- Collected 140 data surveys and established Process Register
- Developed Data Subject Rights Procedure and Request Register
- Designed GDPR Compliance Program
- Updated U-M privacy notice and developed privacy statement
- Prepared GDPR-specific contract addenda
- Developed and implemented cookie consent model
- Created GDPR Toolkit

The GDPR Project kicked off in January 2018. It was staffed with 3 legal experts, 1 analyst, and 1 project manager. The project team was aided by a GDPR working group of representatives from key U-M areas in administration, research, and academic units.

The U-M GDPR Toolkit

- GDPR Self Assessment
- Automated GDPR Data Survey
- Privacy Notice Template
- GDPR Contract and Consent Language
- Cookie Consent Banner Code

The GDPR Project kicked off in January 2018. It was staffed with 3 legal experts, 1 analyst, and 1 project manager. The project team was aided by a GDPR working group of representatives from key U-M areas in administration, research, and academic units.

Privacy Statement

The U-M Privacy Notice is designed to explain how we collect, use, and share personal information. This section provides an overview of the information we collect and how we use it.

Overview

In principle, the U-M strives to:

1. Protect personal information through appropriate physical and technical security measures tailored to the sensitivity of the personal data.
2. Comply with applicable laws, policies, and procedures.
3. Provide opportunities to control your personal information, as permitted by applicable United States and other laws.
4. Consider privacy principles in the design, implementation, and operation of systems that collect or use personal information.

Scope

The U-M Privacy Statement is generally applicable to activities conducted by the University of Michigan that involve the processing of personal information. It is meant to provide a broad overview of the activities that require the processing of personal information and our approach to protecting privacy. U-M Schools, Departments, Units, Clusters and other groups may have Privacy Statements tailored to their specific collection and processing of personal information practices.

Categories of Personal Information We Collect and Use

We identify personal information as any information that relates to an identified or identifiable individual. We generally collect personal information in the following circumstances:

- When you directly provide it to us.
- Through automated processes (for example, through use of learning management tools, or interaction with our websites).
GDPR TOOLKIT

Toolkit: General Data Protection Regulation (GDPR)

If your U-M unit collects and uses personal data, use this toolkit to assess your processes and address General Data Protection Regulation (GDPR) requirements. This toolkit is part of GDPR Compliance at U-M.

First, Determine if GDPR Applies

Answer four questions to help you determine whether the GDPR applies to your data. See Assessment: Does GDPR Apply?

If It Does, Submit U-M GDPR Data Survey

If you believe the GDPR applies to the data you are collecting and processing, please provide additional information to the University’s Data Protection Officer (DPO) by completing the GDPR Data Survey in the Google Form. U-M logon required.

Privacy Statements, Notices, and Templates

The University of Michigan recognizes and values the privacy of the university community members and its guests. Our privacy statement and notices reflect our commitment to privacy and comply with the GDPR.

- U-M Privacy Statement (a general statement on how the university protects privacy)
- U-M Website Privacy Notice (a version of the statement that is specific to the umich.edu website)

U-M units and departments are encouraged to clearly disclose the collection and processing of personal information in a timely manner using these tools:

- Download Unit Privacy Notice Template (MS Word)
- U-M Cookie Consent and Disclosure Banner

General Consent Language

The standard Institutional Review Board for Health Sciences and Behavioral Sciences (IRB/IRBS) consent language has been updated to meet GDPR requirements. We are actively working to update the clinical trial consent language as well. Please work with your IRB to obtain the latest version, as applicable.

If you need specific consent language for a non-IRB-related website, form, or other project, contact us at gdpr.compliance@umich.edu, and we will help you craft GDPR-compliant language.

Contract Addenda

Standard GDPR addenda are available for you to include in U-M contracts as needed. Work with Document Services to ensure your contracts address GDPR requirements where appropriate.

www.safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/policies-regulations/gdpr-toolkit
GDPR Since May 25 in Facts and Numbers

- Nothing substantial yet from a U.S. or higher ed perspective
  - The ICO investigated the possible involvement of the University of Mississippi in the Facebook/Cambridge Analytica case, but found no evidence that UK citizens’ data were transferred to the University (See the ICO Report for the UK Parliament, November 6, 2018)
- European Data Protection Board (EDPB) announced it has 162 active cross-border cases as of October 2018

GDPR Since May 25 in Facts and Numbers

- A Portuguese hospital was fined €400,000 due to lack of technical and organizational methods to protect personal data (fake accounts were discovered in the Case Management system, could have exposed personal data) - biggest fine under the GDPR to date
  - Hospital is challenging the fine against the DPA in Portugal
- According to the EDPB, DPAs received about 18,000 breach notifications by October
- CNIL announced 24,500 organizations from France reported they appointed a DPO
What We Have Learned

- Secure executive support for GDPR compliance
- This is not a technology project
- This is not an IT security project
- Establish partnership with Office of General Counsel
- Engage key stakeholders from across the university
- Focus on processes with highest exposure to GDPR: admissions, alumni engagement, research, international programs
- Provide education, self-service templates, and tools
- Understand this is a long-term commitment to privacy as a value