General Data Protection Regulation (GDPR) Compliance: What You Need To Know And Do

Alexander (Sandy) R. Bilus
Saul Ewing Arnstein & Lehr LLP

June 12, 2018

SAUL EWING
ARNSTEIN
& LEHR LLP

SAUL EWING
ARNSTEIN
& LEHR LLP

Today's Discussion

- Overview
- Why Does This Apply To Me?
- Key Terms
- The Principles of Processing
- The Rights of Data Subjects
- The Responsibilities of Controllers
- Additional Considerations
- Compliance Plan

The GDPR

- New EU law that applies to the "processing" of "personal data"
- Adopted in April 2016, went into effect on May 25, 2018
- Potentially massive fines (up to 20 million EUR or 4% of total worldwide revenue)

Why Does This Apply To Me?

- The GPDR likely applies if:
  - You are established in the EU,
  - You offer goods or services to individuals "in the Union," or
  - You monitor the behavior of people in the EU.
- Examples: study abroad programs, international students and employees, fundraising, marketing, research

SAUL EWING ARNSTEIN & LEHR LLP

Key Terms

- "Personal data" = any information relating to an identified or identifiable natural person ("data subject")
- "Identifiable natural person" = one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
  - Similar to "Personally Identifiable Information" under FERPA
- "Processing" = any operation which is performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, restriction, erasure or destruction
- "Controller" = the person or entity that determines the purposes and means of the processing of personal data
- "Processor" = person or entity that processes personal data on behalf of the controller

SAUL EWING ARNSTEIN & LEHR LLP

SAUL EWING
ARNSTEIN
& LEHR LLP

Principles of Processing

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality

What are the legal bases?

1. Consent (most frequent?)
2. Necessary to protect ***vital*** interests of an individual (emergency contact info)
3. Performance of a contract with the subject (also anticipation of entering into a contract)
4. Legal compliance
5. Public tasks (must be proportionate)
6. Legitimate interest except where interests are overridden by privacy considerations

SAUL EWING ARNSTEIN & LEHR LLP

Data Subject Rights

- Transparency
- Access
- Rectification and erasure
- Restriction of processing
- Portability
- Objection

Responsibilities of Controllers

- Appropriate measures designed to implement the data protection principles (policies, notices, consent forms, data security)
- Record-keeping (what do you have, why do you have it, for how long will you have, how do you protect it, to whom will it be disclosed)
- Relationships with third party vendors (contracts, due diligence)
- Data breach notifications (72 hours to authorities; without undue delay to data subject)

Additional Considerations

- Data relating to children (under 16 years old)
- Special categories of personal data (race, ethnicity, religion, biometrics, health, sexual orientation)
- Criminal convictions and offenses
- Research
- Transfers of data to a country outside the EU

SAUL EWING
ARNSTEIN
& LEHR LLP

Compliance Plan

SAUL EWING
ARNSTEIN
& LEHR LLP

Compliance Plan

- Create a data inventory
- Create privacy notices and consent forms
  - Not just for your website
- Create policies and procedures
- Training

The Data Inventory

- What programs/activities do you conduct that have connections to the EU?
- What personal data do you collect and maintain that relates to EU residents?
- How do you use that data?
- What do you say to individuals about that data collection and use? (i.e., privacy notices, consent forms)
- What third parties do you use to process that data?
- Do you transfer any data from the EU to the US?

The Data Inventory

- Sources
- Systems
- Vendors
- Other Third Parties
- Contracts
- Application Forms
- Current Notices

The Data Inventory

- IT
- HR
- Admissions
- Registrar
- Financial Aid
- Study Abroad
- Distance (Online) Learning
- Marketing
- Advancement

Data Inventory Snapshot

Activity	Type of Data	Lawful basis	And more…
Foreign travel			
Study Abroad	PD of students	Contract	
Sponsored Travel	PD of faculty, staff, and students	Contract	
Marketing and outreach			
Advertising emails/messages	PD of recipients and responders	Legitimate interest	
Research			
Research data sets	PD of EU research subjects	Consent	
Research conducted in EU	PD of EU research subjects; PD of study personnel in EU	Consent	

Notices, Forms, and Contracts

- Privacy notices
  - Required when personal data obtained from data subject and when personal data is obtained from third party.
  - Provide identity and contact info for controller, purpose of the processing, legal basis for the processing, recipients of the data, data retention info, info on transfers outside the EU
- Consent forms
  - Must be written, using “clear and plain” language
  - Don’t default to consent as the legal basis for processing
- Contracts with third party vendors

Policies and Procedures

- Responding to requests to exercise GDPR rights
- Record-keeping
- Incident response
  - Data breach notifications must be provided to regulators within 72 hours and to affected data subjects without undue delay

SAUL EWING ARNSTEIN & LEHR LLP

Looking Ahead

- Training staff
- Maintaining and updating the data inventory
- Evaluate compliance and conduct gap analyses

SAUL EWING
ARNSTEIN
& LEHR LLP

Hypothetical

1. Anna, a student at American College, is studying in Paris for the summer via the College's study-abroad program. Bob, from United States University, also is studying in Paris via American College's program.
2. Anna accuses Bob of sexual assault; files a police report and gets a PFA. Bob sues for defamation; also gets a PFA.
3. Title IX coordinators ask resident director to implement interim measures.
4. Bob claims violation of privacy rights because local resident director transferred personal data to the US without Bob's consent.

Hypothetical—notes

- Resident director in a no-win situation?
- EU/local law will prevail
  - But you have Title IX concerns at home!
- Can get prior written consent
  - BUT consent can be withdrawn . . . **any time!**

SAUL EWING
ARNSTEIN
& LEHR LLP

Questions?

Alexander (Sandy) R. Bilus
Saul Ewing Arnstein & Lehr LLP
Philadelphia, Pennsylvania
215.972.7177
Alexander.Bilus@saul.com

SAUL EWING
ARNSTEIN
& LEHR LLP

Baltimore
Lockwood Place
500 East Pratt Street, Suite 900
Baltimore, MD 21202-3171
T: 410.332.8600 • F: 410.332.8862

Boston
131 Dartmouth Street
Suite 501
Boston, MA 02116
T: 617.723.3300 • F:617. 723.4151

Chesterbrook
1200 Liberty Ridge Drive
Suite 200
Wayne, PA 19087-5569
T: 610.251.5050 • F:610.651.5930

Chicago
161 North Clark
Suite 4200
Chicago, IL 60601
T: 312.876.7100 • F: 312.876.0288

Fort Lauderdale
200 E. Las Olas Blvd.
Suite 1000
Fort Lauderdale, FL 33301
T: 954.713.7600 • F: 954.713.7700

Harrisburg
Penn National Insurance Plaza
2 North Second Street, 7th Floor
Harrisburg, PA 17101-1619
T: 717.257.7500 • F: 717.238.4622

Miami
Southeast Financial Center
200 S. Biscayne Blvd., Suite 3600
Miami, FL 33131
T: 305.428.4500 • F: 305.374.4744

New York
555 Fifth Avenue, Suite 1700
New York, NY 10017
T: 212.672.1995 • F: 212.372.8798

Newark
One Riverfront Plaza
Newark, NJ 07102
T: 973.286.6700 • F: 973.286.6800

Philadelphia
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2186
T: 215.972.7777 • F: 215.972.7725

Pittsburgh
One PPG Place
30th Floor
Pittsburgh, PA 15222
T: 412.209.2500 • F:412.209.2570

Princeton
650 College Road East, Suite 4000
Princeton, NJ 08540-6603
T: 609.452.3100 • F: 609.452.3122

Washington
1919 Pennsylvania Avenue, N.W.
Suite 550
Washington, DC 20006-3434
T: 202.333.8800 • F: 202.337.6065

West Palm Beach
515 N. Flagler Drive
Suite 1400
West Palm Beach, FL 33401
T: 561.833.9800 • F: 561.655.5551

Wilmington
1201 North Market Street
Suite 2300 • P.O. Box 1266
Wilmington, DE 19899
T: 302.421.6800 • F: 302.421.6813

SAUL EWING
ARNSTEIN
& LEHR LLP