UNIVERSITY
OF MIAMI

European Union General Data Protection Regulation (GDPR)

Audit & Advisory Services
University Compliance Services

Resource: CEB/Gartner, 2017

UNIVERSITY OF MIAMI

EU vs. US Approach to Privacy

- **Fundamental Rights:** The word “privacy” does not appear in the U.S. Constitution, so ideas about the concept of privacy have developed over time in the courts. In general, the courts have focused on the idea of privacy as protection from the government.
- **Laws**: In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead, the US has a patchwork system of federal and state laws, and regulations that can sometimes overlap, dovetail and contradict one another.
- **State by State:** States in the U.S. have different privacy laws.
- **Regulatory Powers:** U.S. regulators can take action if companies violate one of the separate laws on sensitive data. In general, the U.S. relies on the Internet industry to regulate itself by agreeing to certain standards.

- **Fundamental Rights**: EU law explicitly enshrines privacy as a fundamental right.
- **Laws**: The General Data Protection Regulation (GDPR) was passed in April 2016 and is meant to harmonize the privacy laws in each EU country and provide a “one stop shop” for companies operating across the EU.
- **Country by Country**: While all members of the EU must comply with GDPR requirements, it may be possible for EU countries to impose stricter requirements.
- **Regulatory Powers**: National data protection authorities (DPAs) in the EU have been given wide-ranging powers to enforce compliance with GDPR, ranging from the power to order the controller or processor to comply with a data subject’s request, to the power to impose a ban on data processing.

Sources: “Should the U.S. Adopt European-Style Data-Privacy Protections?” The Wall Street Journal, March 2013; Hunton & Williams Privacy & Information Security Law Blog, The EU General Data Protection Regulation, December 17, 2015; Practical Law, Data Protection in the United States: overview, July 1, 2015.

UNIVERSITY OF MIAMI

What is the GDPR?

Overview of GDPR

GDPR is the most significant global privacy regulation passed in the last 20 years

- For more than four years, EU authorities have been working on a complete overhaul of EU data protection rules.
- The GDPR replaces EU Directive 95/46/EC, which was passed in 1995 when the internet was still in its infancy.

“GDPR” = General Data Protection Regulation

Who does GDPR apply to?	All companies that handle EU citizen data (customers or employees)
Is GDPR final yet?	YES! The EU Parliament approved the text on April 14 , 2016.
When did it go into effect?	Mid-May 2016, but companies have 2 years to comply. Full enforcement begins May 25, 2018.
What has changed?	A LOT! Next page provides more information

UNIVERSITY OF MIAMI

Additional Background Information

- The General Data Protection Regulation (GDPR) was formally approved by the European Parliament on **April 14, 2016**
- The GDPR replaces the **Data Protection Directive 95/46/EC**, which was originally adopted to regulate the processing of personal data within the EU
- The new rules are designed **to harmonize data protection across EU nations** and will affect all companies that handle the data of EU citizens
- While companies have **two years to comply (Spring 2018)**, many of the requirements will require significant operational changes

UNIVERSITY OF MIAMI

Overview of GDPR Requirements

The GDPR replaces the Data Protection Directive 95/46/EC.

- All companies that handle EU citizens' data are subject to the new GDPR requirements.

Key Operational Requirements

1. **Data Protection Officer (DPO)**
   The DPO assists in monitoring internal compliance with this regulation, managing IT processes, data security.
2. **Breach Notification**
   Companies now have a 72-hour window after discovering a data breach to information national regulators
3. **Privacy Impact Assessments (PIAs)** All "high-risk" data processing activities require privacy impact assessments to be conducted.
4. **Data Subject Consent**
   Data subjects must consent to the types of data collected and how it will be used. Data subjects are allowed to withdraw their consent.
5. **Cross-Border Data Transfers**
   Data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection is acceptable.

New Rights for Data Subjects

Right to Data Portability
A person can transfer his or her personal data from one electronic processing system to and into another without being prevented from doing so by the data controller.

Right to Erasure
This provides that the data subject has the right to request erasure of personal data on many grounds, including a case where the interests of the company is overridden by the interests or freedoms of the data subject.

Deep Dive on New Requirements

While companies have **2 years** to comply with these new requirements, many of them require significant operational reform. Below are the key changes:

- **Appointment of a Data Protection Officer (DPO):** The DPO must assist the controller or processor to monitor internal compliance with this regulation. The DPO is also expected to be proficient at managing IT processes, data security, and other business issues related to the holding and processing of personal and sensitive data.
- **Breach Notification**: Companies now have a 72-hour window after discovering a data breach to information national regulators. The only exception to this rule is if the company demonstrates that the breach is unlikely to result in a risk for the rights and freedoms of individuals.
- **Privacy Impact Assessments (PIAs):** All “high-risk” data processing activities (e.g., surveys, websites, data analytics) will require privacy impact assessments to be conducted. Specific criteria for which activities constitute “high risk” is not yet clear.

UNIVERSITY OF MIAMI

New GDPR Requirements (Cont'd)

UNIVERSITY OF MIAMI

- **Data Subject Consent**: Data subjects must consent to the types of data collected and how it will be used. Data controllers must be able to prove consent and must allow data subjects to withdraw their consent.
- **Cross-Border Data Transfers**: Data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection is acceptable; otherwise, an alternative mechanism must be used (e.g., model contract clauses).
- **Right to Erasure** (a new right created by GDPR): Formerly known as the "right to be forgotten," this provides that the data subject has the right to request erasure of personal data related to him or her on any of a number of grounds that includes a case where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data.
- **Right to Data Portability** (a new right created by GDPR): A person shall be able to transfer his or her personal data from one electronic processing system to and into another without being prevented from doing so by the data controller. The data must be provided by the controller in a structured and commonly used electronic format.

UNIVERSITY OF MIAMI

Why Should We Care?

For the first time, companies will face significant monetary fines for violating the GDPR requirements.

Sanctions can range from the greater of **2% of a company's global revenue** or **€10 million** for certain violations to **4% of global revenue** or **€20 million** for other offenses.

$15 Billion in 2016 global revenue* **X** **4% sanction** for GDPR Violation **=** **$600 Million** fine

*Note: $15 Billion represents the median member company annual revenue for 2016.

UNIVERSITY OF MIAMI

GDPR Action Plan

Do Now

- ☐ Appoint a Data Protection Officer
- ☐ Implement PIA Program
- ☐ Expand Breach Response Protocols
- ☐ Identify Cross-Border Data Transfers
- ☐ _____
- ☐ _____

Do Next

- ☐ Address new substantive rights created by GDPR

Develop necessary training and communications

- ☐ _____
- ☐ _____
- ☐ _____

Additional Information

Nelson Perez, University Compliance Services
E-Mail: nelsonperez@miami.edu
Phone: (305) 284-2924

GDPR Webpage
https://compliance.miami.edu/focus_areas/gdpr/index.html

Helenmarie Blake, Esq.
Chief Privacy & Data Integrity Officer
E-Mail: hmb33@miami.edu
Phone: (305) 243-5000

UNIVERSITY OF MIAMI