

# The Time is Now: Prepare for the EU's New Data Privacy Act Rule

As of May 25, 2018, many companies who collect, host or otherwise process or monitor the personal data of EU residents will need to comply with the EU's new comprehensive data security and privacy law known as the General Data Protection Regulation (GDPR). While primarily designed to harmonize data privacy laws across the EU, the law also reaches beyond the EU and can apply to companies operating entirely outside of the EU. For many U.S. based companies, the GDPR's requirements vary significantly from data privacy obligations they may owe to individuals in the United States.

## Who Does It Affect?

Any company, regardless of whether it has a physical location within the EU, which collects, hosts or otherwise processes the personal data of EU residents will likely need to comply with the GDPR. The GDPR creates obligations for non-EU-based companies if they (1) offer goods/services to or monitor the behavior of individuals located in the EU residents, and (2) process the personal data of those individuals.

## What is Personal Data?

The GDPR broadly defines "personal data" to include any information that can be used to directly or indirectly identify the person. Personal data can include someone's name, email address, bank information, a photo, financial account information, credit card number, medical information, social networking posts and any other information that can be traced back to an individual. Personal data also includes technical information, such as, IP addresses, cookies, or other electronic identifiers that may be used to identify a person. In effect, the collection, processing, use, or storage of any information that contributes to identifying a person may trigger the obligations and liabilities of the GDPR.

## What Does "Processing Mean"?

Similarly, the term "processing" is defined expansively. Processing means any operation performed on personal data, such as collecting, recording, storing, using, disseminating or deleting. It includes the collection of any identifying

### POSTED:

Jan 25, 2018

### RELATED PRACTICES:

#### [Corporate Law](#)

<https://www.reinhartlaw.com/practices/corporate-law>

#### [Labor and Employment](#)

<https://www.reinhartlaw.com/practices/labor-and-employment>

### RELATED SERVICES:

#### [Data Privacy and Cybersecurity](#)

<https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity>

#### [Inbound Foreign Investment](#)

<https://www.reinhartlaw.com/services/inbound-foreign-investment>

#### [Food and Beverage](#)

<https://www.reinhartlaw.com/services/food-and-beverage>

#### [International](#)

<https://www.reinhartlaw.com/services/international>

#### [Commercial and Competition Law](#)

<https://www.reinhartlaw.com/services/commercial-and-competition-law>

### RELATED PEOPLE:

#### [Derek H. Campbell](#)

<https://www.reinhartlaw.com/people/derek-campbell>

#### [Martin J. McLaughlin](#)

<https://www.reinhartlaw.com/people>

information of individuals located in the EU, such as logging IP addresses of website visitors or tracking cookies from their computers. Thus, a business can become subject to the GDPR without any actual sales to EU residents if sufficient monitoring or marketing occurs. Therefore, a business could trigger GDPR compliance requirements if its website collects IP addresses of individuals located in the EU.

## What Does the GDPR Require?

Companies falling within the purview of the GDPR must satisfy a lengthy list of obligations. For example, companies that collect or process personal data must obtain active and informed consent from the data subject (i.e., the individual) prior to collection. If the collection or processing of personal data is for multiple purposes, consent must be obtained for each purpose. Explicit consent (i.e., the individual's actual opt-in to the processing) is required if certain sensitive personal data is collected. As a practical matter, these specific consent and disclosure requirements will require many companies to update, clarify and expand their existing privacy policies.

Data subjects also have the right to access their personal data to verify the lawfulness of the processing and the data's accuracy. Additionally, if a company uses personal data for direct marketing purposes, the GDPR grants data subjects the right to object, and requires companies to explicitly inform people of that right. Further, if a data breach occurs, the GDPR generally requires notification to the relevant authorities within 72 hours of the discovery thereof.

## What Are the Risks of Noncompliance?

Fines for violating the GDPR are significant. A company can be fined up to the greater of 4% of its annual worldwide turnover or €20 million.

## What Should You Do?

If you believe your company may be affected by the GDPR, speak with someone knowledgeable about the GDPR as soon as possible. For many companies, becoming compliant will require the active participation of personnel from several departments (e.g., IT, legal, HR, etc.), outside consultants and advisors.

In order to achieve compliance, most companies will need to undertake a comprehensive review of their information security and data collection practices,



including:

- Updating privacy policies to ensure they provide for an individual's unambiguous, informed consent to the specifically identified data collection activities;
- Evaluating and mapping their data flows and collections;
- Updating incident response and data breach plans;
- Revising third-party and vendor contracts to ensure third party compliance;
- Evaluating whether the appointment of data protection officers is required; and
- Reviewing whether to adhere to the EUUS Privacy Shield Framework to comply with data transfer requirements applicable to the transfer of personal data from the EU to the United States.

*These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.*