

GDPR Enforcement Coming Soon

May 9, 2018

By now, you are likely to have heard that enforcement of the European General Data Protection Regulation (GDPR) is starting soon.

Because the change is so significant, it can be a bit overwhelming to consider how the new regulations may impact your business or your clients' businesses. To help, we recently hosted a training session at Miller Canfield, which you may view by [clicking here](#). Additionally, we summarize the GDPR and its impact below.

A few frequently asked questions include:

What is the GDPR?

The General Data Protection Regulation, or GDPR, is a set of rules enacted in the European Union, setting new and higher standards for privacy rights of individuals located in the EU and obligations imposed on controllers and processors either located in the European Union or located outside, but to which the GDPR applies. It is consistent throughout EU member countries and will have a global impact. The regulations were enacted on April 26, 2016; enforcement begins on May 25, 2018.

Your Business is in the U.S. Will You Have to Do Anything?

Yes. Anyone who offers goods and services to individuals located in the EU and anyone who monitors their behavior as long as such behavior takes place in the EU will need to comply with the GDPR.

Noncompliance penalties can be steep. Running afoul of the GDPR could lead to fines of up to 4 percent of a company's revenue or €20 million (whichever is higher). Additionally, individuals who are affected may sue the data controller or data processor or both.

What are Data Controllers and Processors?

In short, a data controller is an organization or person that determines the purposes and means of the processing of personal data. A data processor is a person, authority or agency that processes personal data on behalf of the controller.

What Data is Covered in the GDPR?

Any information that relates to identified or identifiable individuals, regardless of the way it is being processed. It includes, among others:

- Name
- Address

Continued

- Email Address
- IP Address
- Location Data
- Online Identifier
- Genetic and Biometric Data
- Medical Information
- Sexual Orientation
- Race and Ethnicity
- Political Opinions
- Religious or Philosophical Beliefs

What are the New Rights and Responsibilities?

There are 99 articles and 173 recitals defining privacy rights of individuals and the obligations of controllers and processors of data.

Individuals' rights include:

- Right to have inaccurate personal data rectified
- Right to be forgotten
- Right to receive their personal data
- Right to obtain from the controller restriction of processing
- Right to object to processing of personal data
- Right to revoke consent at any time
- Right for data to be securely stored and transferred
- Right to have outdated data erased

Responsibilities include:

- Companies that employ more than 250 people must document why individuals' data is being collected and processed. They must describe how the information is being collected, processed and stored.
- Companies must describe security measures to protect stored personal data.
- Data collectors must obtain consent to collect and process personal data. They must clearly describe what data is being collected and how it will be used and provide a "positive opt-in" from the consumer.
- Privacy policies must be easy to understand and must provide individuals with the information they need to make informed decisions regarding their data.

Continued

- Companies that regularly and systemically monitor individuals' data must hire a data protection officer.
- In the event of a breach, companies must notify appropriate regulators within 72 hours.

What Should You Do Now?

If you have not already done so, you must immediately conduct an assessment of your privacy policies and contracts to ensure that they are compliant. The Information Commissioner's Office in the UK has offered a checklist to help in preparation and compliance with GDPR. It includes:

- Make sure that key people in your organization are aware of the law.
- Document what personal data you collect and store, where it came from and who you are sharing it with.
- Review privacy notices and make necessary changes.
- Ensure that your procedures cover all of the new rights of individuals, including how you would delete personal data.
- Review how you seek, record and manage consent and determine what changes you need to make.
- Ensure that you have adequate procedures in place to detect, report and investigate a data breach.

For assistance and advice on compliance and the applicability of the GDPR for U.S. entities and assistance with drafting or review of privacy-related documents, please contact a Miller Canfield attorney to discuss your needs.