GDPR Series, Part 1: Does the GDPR Apply to You?

Generating much interest (and concern) globally is the European Union General Data Protection Regulation (GDPR), the successor to the Data Protection Directive (95/46/EC). Enforcement is slated to begin in May 2018, and those not in compliance can expect very stiff financial penalties. In the meantime, companies should revisit their security and compliance strategies to ensure they're prepared to meet GDPR requirements.

This is the first in a series of four blog posts examining the GDPR, specifically:

- To whom the GDPR applies
- The key data security requirements of the GDPR
- Organizational implications of the GDPR
- The penalties for non-compliance

To start, let's review some definitions that are core to the GDPR.

Key Terms

Personal data and data subject

This is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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 natural person."[1]

Example: You work at a Fortune 500 company and as your employer it holds your personal data. You're the data subject.

Controller

This is a "person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[2]

Example: A manufacturing company collecting personal information from its employees is the Controller.

Processor

This is a "person, public authority agency or any other body which processes personal data on behalf of the controller."[3]

Example: A payroll company processing employee paychecks on behalf of the manufacturing company is the Processor.

To Whom Does the GDPR Apply?

Non-EU companies and entities may believe that the GDPR doesn't apply to them. Simply put, it may.

GDPR requirements apply to any organization doing business in the EU or that processes personal data originating in the EU, be it the data of residents or visitors.

So organizations of any size in any country that process anyone's data—if that data originated in the EU—is subject to the GDPR.

GDPR Requirements Stick to the Data

The borderless realms of the internet mean that companies not intending to control or process EU-sourced data could find out they are subject to GDPR requirements.

Consider these scenarios:

You're part of a financial analyst firm tasked with projecting a European company's revenues for the next three years. You work out of an office in the US, but use personal data provided to you by your client that was collected in the EU. Since this data was collected in the EU it is subject to GDPR requirements, even though you're based out of the US office and didn't originally collect the data.

A mobile and on-line website allows people to shop for, buy and rate products. The US-based company that owns the retail storefront collects personal data about the people that visit and make purchases. The information is subsequently used in advertising campaigns and sales reports. If a person visits the website while they are physically present in the EU, the requirements of GDPR follow the personal data collected during their visit. That essentially means that any website or mobile application that is accessible by a person in the EU will need to comply with GDPR.

There are of course allowances for small businesses and practical limitations on what the EU would attempt to enforce. But entities located outside the EU that market their products or do business with people inside the EU will need to consider the ramifications of not complying with GDPR.

Planning Framework

As this was just the first installment of a four-part series on the GDPR, Part 2 will take a closer look at the actual data security requirements. In the meantime, if you're ready to go deeper on planning for the GDPR, review our blog post that provides a GDPR readiness framework including milestones for each stage.

Other Posts in the Series

GDPR Series, Part 2: What Rules Require Data Protection Technology?

GDPR Series, Part 3: Preparing Your Organization for the GDPR

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016