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

So far, in Parts 1 and 2 of our GDPR series, we've covered who is subject to GDPR requirements and what the specific data security requirements are. In this post, we'll look at what the GDPR means for organizations and how to prepare.

Even though enforcement doesn't begin until May 2018, there are some key questions every organization should be asking itself as the enforcement day approaches.

What Data Do You Have and Where is it Stored?

You need to assess what kinds of data your organization currently has under management. This includes identifying what kinds of personal data (e.g., financial information, customer records, employee records, marketing optimization information, etc.) you have and where they are stored — including data stored in cloud-based systems.

Many outside the confines of the darkest recess of the IT department will not realize that creating and maintaining an accurate inventory of the structured and semi-structured data scattered across the entirety of an enterprise is difficult if not impossible to do manually. This task must be automated using tools that can detect unknown data stores and locate personal and confidential data within the data structure based on a variety of pattern recognition techniques. Once found, the information must be classified and assigned a risk profile.

Who Has Access to the Data and Can You Control that Access?

A key data protection requirement is limiting access to personal data, which can be accomplished in several ways including data collection minimization and data masking. Whilst these are both recommended steps, some users and applications will need access to the live personal data. Identifying those applications and users requires user access controls, user rights management and activity monitoring. Like data inventories, these tasks are best automated with technology.

Common gaps in companies' access limits are excessive rights granted to use a privileged application or a service account or access rights that have simply accrued over time. This is where technology powered by machine learning can help close gaps and minimize access.

What Responsibility Do You Have for Your Processors?

If you're a data controller, and you use processors (or sub processors) you need to take steps to ensure that the processors will protect the data you control, in accordance with your GDPR policies. This critical requirement is best addressed by a combination of contracts from your legal team and technology that can enforce limitations on the movement of data.

This is especially important if there is any chance the data could be transferred to and viewed by persons outside the EU or a country recognized as having adequate data protections by the EU such as Israel, Switzerland, Argentina, and New Zealand. The full list of countries with adequate data protections is published by the EU here. Even a remote desktop session via VPN violates the data transfer requirements if the person viewing the data is sitting outside the EU or the countries that have been deemed to have adequate protection. You'll want to have both legal and technical controls in place to monitor and control access to your data.

Chapter V of the GDPR covers transfers of personal data of EU data subjects to third countries or international organizations and mandates that organizations that control or process such data ensure that any such transfers be done with adequate safeguards in place to protect the personal data of EU subjects. If adequate safeguards are not in place, then the data should not be transferred.

What About Data Transfers from the EU to the U.S.?

A simple question: can your organization control its data if it enters the U.S.? Model contracts and Binding Corporate Rules (BCRs) will help some companies address specific controller-processor relationships. Companies that cannot utilize these contracts relied on the Safe Harbor Framework to provide a legal basis for data transfers to the U.S. The Safe Harbor Framework was invalidated in 2015, but it was replaced by the EU-U.S. Privacy Shield Framework in 2016.

The Privacy Shield Framework was designed by the U.S. Department of Commerce and the European Commission to provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States. The Privacy Shield Framework utilizes a self-certification format and is open to U.S.-based organizations. Once an eligible organization makes a public commitment (via the Privacy Shield website) to comply with the framework, the commitment will become enforceable under U.S. law.

Although debate still continues as to whether the Privacy Shield Framework will pass muster in the face of a legal or regulatory challenges, as of now it has credibility given that, as of March 1, 2017, 1,750 organizations — including Facebook, Google, Microsoft, Oracle, and Salesforce — have joined the EU-U.S. Privacy Shield[1] and it has been approved by the European Commission.

What to Do First?

GDPR compliance may seem daunting initially, but if you can answer the questions above, you're already off to a good start. At a high level, your responses will help you build a preliminary plan along the following lines:

- Identify what kinds of data you have, where it's stored and its risk profile
- Examine the data flow and all the access points
- Assess current protection policies and procedures
- Perform a prioritized gap analysis to the new requirements
- Identify technology, processes, contracts, and resources to address the gaps
- Work back from the May 2018 enforcement date to determine your timeline for rolling out the new elements.

This is just the starting point and is not meant to be a comprehensive list. Visit our blog post on GDPR planning for additional details and a timeline for how to tackle GDPR readiness.

For More Information

White Paper: GDPR: New Data Protection Rules in the EU

Breach Prevention: Protect Your Data from Insider Threats

Data Masking: Reduce the risk of non-compliance and sensitive data theft

Other Posts in the Series

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

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

GDPR Series, Part 4: The Penalties for Non-Compliance

[1] https://www.privacyshield.gov/list