100(ish) Days Until GDPR
by Reggie Pack

In a little more than 100 days (May 25th, 2018), a sweeping regulation known as the General Data Protection Regulation (GDPR) will go into effect across the European Union. The purpose of the GDPR is to update and modernize the scope of protections that are placed on "personal information" stored about individuals by certain entities. The regulations are broad and include significantly increased requirements and associated penalties for non-compliance. As but one piece of evidence regarding how seriously the EU is taking the GDPR, these new regulations are included within the broader "EU Charter of Fundamental Rights."

A brief overview of the GDPR is provided below. Additionally, some explanation is also included as to why the GDPR is important even to U.S. only companies.

WHO IS AFFECTED BY THE GDPR?

The GDPR applies to "all companies processing and holding the personal data of data subjects residing in the European Union, *regardless of the company's location*."

In other words, even if you are a U.S. based company, if you store customer information, client information, sales-lead information, contact information, or other "personal data" about any person who resides in the European Union, you are responsible to abide by the GDPR with respect to any business operations that occur within the EU.

WHAT CONSTITUTES PERSONAL DATA?

In the United States, a more common term for sensitive data is "personally identifiable information" (PII). In the U.S., PII has historically been limited to data that can be directly linked to a particular person. For example, names, addresses, social security numbers, etc., have been treated as PII. Other information about individuals such as birthdates, telephone numbers, email addresses, etc., have traditionally been treated as non-sensitive information and have, subsequently, rarely been subject to regulation. Under the GDPR, personal data includes **"any information related to a natural person that can be used to directly *or indirectly* identify the person."**

The inclusion of “indirect” data likely broadens the reach of GDPR protections dramatically. As data analytics technology improves, the ability to derive identifying information from sets of previously “non-sensitive” data has become easier and easier. For example, knowing only a birthdate, gender, and zip code can allow direct identification, by name, of large portions of a population. Likely because of this, the applicability of the GDPR is not based on any distinction between “sensitive” personal data and any other personal data.

WHAT IF I DON’T COMPLY?

The GDPR states that a company can be fined up to 4% of their total annual revenue, up to 20 million euros, for failing to comply with the GDPR. While non-compliance is likely to be discovered in conjunction with a breach or data incident, penalties under the GDPR are not limited to circumstances where data is actually exposed. And although the 20-million-euro maximum penalty is likely to be reserved for egregious and willful violations where actual data is exposed, penalties may be levied simply for discovered non-compliance even without a known data exposure. As such, the penalties imposed by the GDPR greatly exceed any previous data privacy regulation regimes.

WHAT DOES THE GDPR REQUIRE ME TO DO?

The GDPR is broad and complicated. Some requirements vary depending on the degree an entity controls, processes, or stores personal data. However, some general principles apply to all entities covered by the GDPR.

Consent

First, consent requirements have been strengthened. While the GDPR applies to all entities that collect *any* personal data, consent requirements do differ according to the type of personal data being collected. Generally, more sensitive data requires “explicit” consent to collect (e.g., specific consent for the particular data item to be collected.) As such, collection of more sensitive data must inherently be “opt-in.” Less sensitive data, however, requires

only “unambiguous” consent. Regardless of the type of data being collected, the GDPR also requires that “opt-out” procedures be as clear and easy for a person to choose (even at a later date) as “opt-in” options are.

In practice, this means that covered entities likely need to revisit privacy policies, shrink-wrap/clickwrap provisions, contracts, and other disclosures to ensure both the specific types of data that are collected are identified and, perhaps more importantly, that such documents are clear and easy for a person to understand. Additionally, entities should also be concerned about *where* those clauses are found within agreements, including considering whether data collection provisions should be excised from larger agreements and separately presented to users to ensure that the “explicit” consent requirement is met.

Good practice also dictates that consent is periodically verified and updated to lessen the likelihood of assertions of non-consent if/when a data incident occurs.

Reporting

Second, data breach reporting requirements have also been strengthened. Generally, the standard within the U.S. (mostly dictated by state law), is that breaches must be reported: “within a reasonable timeframe.” The GDPR instead introduces a role known as a “Data Protection Authority” (DPA). Any entity that experiences a loss of data (e.g., a breach, malfunction, inadvertent disclosure, etc.) is required to report the incident to their DPA within 72 hours of learning of the incident.

DPAs have been established in various EU member states to receive such reports. For example, a French company reports a breach to the French DPA, and a German company to the German DPA. For entities covered by the GDPR but that are not organized with the EU (e.g., U.S. based corporations collecting personal data of EU residents for business purposes within the EU), the reporting requirements are more complicated. The entity may be required to report to the DPAs corresponding to the residencies of the people affected by the data incident. As such, incidents must be recognized and quickly analyzed to identify the proper DPAs to contact within the 72-hour reporting window.

Data Protection Officer
Third, depending on the degree to which your company is involved in personal data collection and/or processing, you may be required to establish/assign a Data Protection Officer. In many cases, a DPO may serve multiple roles within an organization, but as the quantity and sensitivity of collected data increases, the more beneficial it may be to have a dedicated DPO assigned to track and manage data activities within your company.

Finally, while the GDPR is *mostly* a European Union concern, there are strong indications that similar shifts in data privacy regulations are likely to make their way into U.S. law either on a state-by-state manner or as some eventual Federal data privacy regulation. So, while the GDPR may not apply to your organization yet, it is likely that similar types of rules may eventually be required. To that end, understanding the GDPR and proactively preparing your organization for eventual changes is likely wise business strategy.

ADDITIONAL RESOURCES:

Full Text of the GDPR:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Home Page for EU Data Protection Information
https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en