# The EU's Data Protection Deadline Means Business

2.12.2018

**The EU's Data Protection Deadline Means Business**

You may not have been paying attention to the upcoming GDPR (General Data Protection Regulation) deadline on May 25th, thinking that it does not apply to your company, but it may.

Here's a simple test:

You are a domestic US company with all staff and data-processing located in the US. Your market focus has been domestic US consumers, but your marketing department recently expanded your offerings (goods and services) to include potential consumers in the EU. So far, you have neither shipped a good nor been retained for services. Does the GDPR apply?

And then there's this twist:

You are a domestic US mobile app developer with your staff and analytics vendor all based in the US. Your app is focused on "foodies"—people who enjoy finding and commenting on new food trends in restaurants. Your app can be downloaded both on Apple and Android devices. Does the GDPR apply?

The answer to both scenarios above is YES.

The data-driven focus of today's global economy is far different from what it was twenty years ago when the EU adopted the Data Privacy Directive.[1] Since then, US companies have learned to accommodate the EU's privacy requirements by self-certifying with the Safe Harbor Privacy Principles finalized in 2000 that were followed by the slightly more stringent, post Edward Snowden-impacted Privacy Shield in 2016. Now business is bracing for the GDPR. In a few short months, the GDPR will go into effect, marking the first comprehensive change to the EU's data privacy regulations since 1995.

## Related Services

Connected Car and Autonomous Vehicles

Cybersecurity and Privacy Specialty Team

Emerging Technology Specialty Team

Privacy, Data Breach & Data Security

*The impact of the GDPR will be extensive and will touch any US company that has either: (i) operations within the EU or (ii) offers goods or services to individuals in the EU.*

While many of the key privacy principles from the 1995 Data Privacy Directive remain, there are some important differences that may catch companies by surprise. Among these differences are those addressing territorial scope, sufficiency of consent, and penalties.

**1. The Increased Territorial Scope**

The GDPR will apply to all companies that process personal data from individuals residing within the EU, *regardless of where the company is located*. This is not really new, but under the 1995 Directive, the issue of territoriality was ambiguous. The GDPR now makes it abundantly clear: with very few exceptions, the GDPR will apply to controllers and processors in the EU when they process personal data from EU residents regardless of where the processing takes place. The bigger territoriality change is that the GDPR now applies to non-EU controllers or processors when they process personal data from EU residents under specific circumstances. This could come as a big surprise to the domestic US company whose marketing reaches across the Atlantic. In addition, those non-EU businesses that process the data of EU residents will have to appoint a GDPR "representative" in the EU.

- **When a Company Monitors EU Citizens**

In this scenario, let's say that a US company decides to launch a mobile app that gathers the location data of its users. The company is based in the US, its staff resides in the US, its third-party analytics vendor and cloud provider are based in the US with servers in the US, but its target market includes millennials in the US and beyond. Thus, even though the company has no base of operations in the EU and does not process the personal data it gathers in the EU, because its social media network monitors the activities of EU millennials, the GDPR will apply.

- **When a Company Targets EU Citizens**

Let's change the facts a bit from the prior scenario: the US company does NOT process data, rather it merely offers a selection of widgets for sale on its US-based website. The widgets are popular and orders come in from all over the world. When those widgets are mailed to EU residents, the GDPR applies. The results are the same if the US company offers a service (whether paid for or not). The key word here is "offers".

**2. The Requirements for Valid Consent**

Proper consent is paramount under the GDPR, and what is meant by "proper" consent could be misunderstood, given the cultural differences on this issue between the US and Europe. Where the European default since the 1995 Privacy Directive has been the"opt-out" approach where one is automatically opted out of receiving something—email updates, notices of new products, you name it —the US default always has been to have that "opt-in" box checked, allowing users to opt out of receiving such notices only if they take the affirmative step to uncheck the box. The GDPR requirement

to obtain clear, unambiguous consent for a plainly defined purpose ***before*** gathering the personal data from an individual will be a heavy lift for many US companies. And once obtained for that one purpose, the data cannot be used for a different purpose not described in the original consent. Processing of the data must be fair, lawful, and transparent.[2] Finally, it must be just as easy for the data subject to withdraw his or her consent as it was to give it.

**3. The Penalties for Non-Compliance**

Fines are stiff and apply to both controllers and processors that are in breach of their obligations under the GDPR. The fines are two-tiered with the lower-level tier set at the greater of €10 million or 2% of the company's worldwide annual revenue from its prior fiscal year. Activities subject to these lower-level fines are failures pertaining to recordkeeping, breach notification, or impact assessment, among others. The higher-level fine can be as much as 4% of the company's worldwide annual revenue or €20 million, whichever is greater. Examples of activities subjecting controllers and processors to these higher-level fines are violations of core privacy by design principles or processing data without sufficient customer consent.

There is much more to the GDPR than can be stated in this one Alert. The technical and legal challenges surrounding the GDPR's requirements can be daunting, thus requiring careful planning and implementation. There are many online resources, but a good place to start is with the website for the European Commission.[3] Of course, we at Butzel Long would be pleased to assist.

**Claudia Rast**

734.213.3431

rast@butzel.com

---

[1] Officially, Directive 95/46/EC.

[2] If no lawful basis exists, the company will be in breach of a core privacy principle.

[3] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.