GDPR Compliance Deadline is May 25, 2018: Privacy Regulation is a Moving Target

05.14.2018 | By Thomas Dover

Worldwide, companies are scrambling to meet the May 25th deadline to comply with the European Union's General Data Protection Regulation (GDPR). For companies with physical operations in an EU member state, this deadline is well-known and preparations should be close to complete.

Qualifying companies will be required to enforce protections for the personal data (personally identifiable information in most US state and federal definitions) of EU citizens including strict requirements for individual consent, the so-called right to be forgotten, 72-hour breach notice, and very high fines (relative to international and US state and federal) that escalate from 2% to 4% of global revenue.

Increasingly, mid-sized US companies are asking: *Do I need to do anything?*

The short answer is **Yes**.

The GDPR[1] requires any entity that collects or processes personal data (including behavioral information) of an EU citizen, and where such personal data is transferred out of the EU, to conform to the new comprehensive guidelines. In order for the GDPR to apply to your company, your company must collect or process personal data of an EU citizen in relation to the offering of goods or services to individuals in the EU. Since most companies have websites accessible by citizens of the EU, every company must audit itself. This process is monumental, time-consuming, and riddled with opportunities to miss relevant personal data. Another factor that needs to be considered is the locations (server, cloud, and laptop) where employees (or vendors) save information. Now panic.

Even if your company does not maintain a physical operation in the EU, you are most likely collecting or processing personal data of EU citizens via your website (or mobile applications, etc.). This is true even if a transaction hasn't occurred. Article 3 of the GDPR clearly indicates that compliance is required if the data

subject (EU citizen) is *in the EU* when the data is collected. While the scope and enforcement of the GDPR is the subject of some speculation, the general analysis is whether your activities (i.e., website) *targets* EU citizens. Having an e-commerce website and the ability to sell and ship anywhere, is not the end of the evaluation.

A few questions to consider:

- Does your website offer non-English language translations?
- Are EU-specific goods or services offered?
- What currencies do you accept?
- Does your website include profiles or successes of EU-based citizens, services or product reviews?
- What if the EU citizen created an account in the US but then accessed their account after returning to the EU?

From simple email marketing to big data analysis and use, the evaluation remains the same. Once your company believes that it may be subject to the GDPR, what should you do? As a practical matter, be compliant.

Since the EU has decided that the US does not maintain an adequate level of protection for personal information (we're in good company since the EU has found less than a dozen countries as adequate), your company can comply with appropriate safeguards. One such safeguard is the US Privacy Shield[2], a certification program managed by the US Department of Commerce.

The Privacy Shield is a voluntary, self-certification program under which a company has illustrated compliance with a variety of processes, notices, and principles. This certification process includes:

- Developing a Privacy Policy (website and otherwise) that conforms to the Privacy Shield principles.
- Making the Policy and Privacy Shield principles available to the public.
- Including mechanisms that allow each citizen to manage, control, and delete their personal information.
- Identifying a data protection agency (DPA) and an arbitration mechanism.
- Designating an individual responsible for the compliance and verification of Privacy Shield principles and directives.

If your company decides to proceed down the path of Privacy Shield certification, keep in mind that you are now subject to the US laws that enforce such compliance. This is true even if you would not have been held to such standards under the GDPR. In addition, your company will be subject to annual compliance certification as well as compliance with new regulations or directives developed after certification of the Privacy Shield.

In broad strokes, the GDPR has set the stage for worldwide protection of personal information. Its approach requires that personal data is:

- Accurate, including accessibility for update/modification/deletion by each individual.
- Secure.
- Transparent regarding use, storage and access.
- Pursuant to direct, active consent of each individual, for each use.

An exhaustive outline of the GDPR requirements would be nearly as long as the 80+ page document itself. Some of the lesser-known aspects, including the limitations on consent (minors), requirements for handling sensitive data and breach notice obligations should be considered on a case-by-case basis. But no matter which approach you choose, make sure you are in compliance with the GDPR requirements. Violations of the GDPR can result in huge fines of up to €10 million, or 2% of a company's global annual turnover.

You can stop panicking.

The GDPR is a beacon and is shining a bright light on the type of information that companies collect and what privacy and permission controls should be in place.

In light of these changes, every company should perform an audit to evaluate its practices and operations focusing on the what, where, when, how and – most importantly - why. This new approach will inform your company's policies well into the next wave of privacy directives and regulation and you will be prepared.

For assistance with GDPR issues, Privacy Shield certification or any related privacy/data security concern, please contact: Thomas Dover or Jim Vorhis.

[1] EU Regulation 2016/679

[2] https://www.privacyshield.gov/