Cooley

GDPR: Ready or Not, Here It Comes…

December 4, 2017

What does the beginning of December mean to you?

The start of the holiday season? Well, yes, but it also marks the start of the 6-month countdown to GDPR. Are you ready? According to the latest statistics, 86% of companies (of all sizes in multiple industries) are not – and over 60% have not even started planning or taken any preparatory steps towards compliance.

Don't worry, if you follow the steps outlined in our 6-month plan below, you can be well on your way to being GDPR-ready by 25 May 2018.

What is the GDPR and why does it matter?

The General Data Protection Regulation (aka "GDPR") is part of a wave of new legislation that is due to come into force on 25 May next year. This, together with other pieces of legislation look set to radically change the use and flow of data worldwide.

The overriding concern (aside from the potential for huge fines) is the GDPR's extra-territorial scope: despite being a European law, a non-European company may need to comply even if it does not consider itself to have an EU "presence". Furthermore, some of the new requirements (legal, technical and operational) are significant and may take time to implement.

Does it apply to me/my business?

You need to ask two key questions:

1. Do you "process" EU data? This is interpreted broadly and can include accessing, storing and transferring. In fact, it is difficult to think of anything an organisation might do with data that will *not* fall within this definition.
2. Does the data constitute "personal data" of EU citizens or residents? This includes data that could identify a person and extends to data which while, in isolation, does not identify a person, would do so when combined with another piece of data. Basically, pretty much anything – not just the obvious, names, email addresses and phone numbers but any data relating to a living person, including online identifiers (e.g., IP addresses, device identifiers, Twitter handles, etc.), location data and a range of sensitive data such as medical data - could be considered personal data. Importantly for US readers, this is broader than PII.

Ok, so it applies, what does it mean in practice?

The new rules around data privacy were born out of both a need to deal with the use of data in a world of new and emerging technologies, together with the desire to provide greater protection of personal data belonging to EU citizens and residents.

The key features – those that will likely have the greatest practical impact – are the following:

- Stronger rights for individuals – higher standard for consent (this may affect privacy policies and online data collection processes); an individual may withdraw their consent and exercise a variety of additional rights
- Processor obligations – entities that handle data on behalf of others have new statutory obligations (plus any imposed by contract)
- EU Representative – some entities based outside the EU may need to appoint one
- Breach notification requirements – new duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected
- Expanded security requirements – systems must be designed with privacy in mind and security must be proportionate to risk
- Accountability – you will be required to keep records of measures used to comply so everything should be documented (e.g. plans, policies and any other materials relating to your handling of personal data)

What happens if I don't comply?

It depends what you classify as your worst-case scenario. It could be a breach of the law, like mishandling data or a data breach, in which case you are looking at reputational damage, business losses and fines of up to €20 million or 4% of worldwide annual turnover (whichever is greater). Or it could be delaying or losing out on an M&A transaction or an investment opportunity because you are not GDPR compliant.

Sounds pretty big, am I too late?

In short, yes it is big but if you start preparing now, you can be ready for when the new rules hit.

Month 1/December 2017: Raising awareness

- Gather a GDPR team (this is a multi-stakeholder issue) and appoint a Data Protection Officer (not always required but advisable) to lead
- Involve management across the organisation and engage the board as soon as possible – allocate budget
- Conduct data protection and cybersecurity training

Months 2–3/January – February 2018: Information gathering/gap analysis

- Conduct GDPR survey: information gathering exercise to identify what personal data the company holds/has access to and where – inventory
- Gap analysis: map data flows against GDPR requirements to identify any gaps
- Develop Implementation Plan: identify and prioritize actions (risk based)

Months 3–6/March – May 2018: Implementation

- Review/prepare/update: privacy policies and other policies; other notices (internal and external); contracts with third parties; internal practices, processes (data handling, data security, incident response) and record keeping
- Seek out GDPR-compliant technology: develop strategies for privacy by design and by default (minimise processing/retention; use encryption and pseudonymisation where possible)

Month 6/May 2018 and beyond: Monitor and Maintain

- Regular training across the business
- Regular monitoring of updated systems, policies and procedures
- Regular (yearly) data protection impact assessment

Key takeaway

Each business, large or small, will face its own personal challenges with regard to GDPR. However, adopting a pragmatic, strategic approach (both operationally/technically and legally) will allow you to use it as an opportunity. In fact, compliance could, if properly managed, drive efficiencies for your business – and at the very least, facilitate the ability to leverage and monetize data as the valuable asset that it is.

Key Contacts

Ann Bevitt London	abevitt@cooley.com +44 (0) 20 7556 4264
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090