Cooley

New Year's Resolution for Edtech Companies: Get Ready for GDPR

January 25, 2018

January 1 means the end of the holiday season and the start of a new year. It also marked the start of the five-month countdown to the European Union's new **General Data Protection Regulation**. If your first question is "What is GDPR?", you are not alone. According to the latest surveys, nearly nine out of 10 companies (of all sizes in multiple industries) are not currently ready for GDPR – and almost two-thirds have not even started planning or taken any preparatory steps towards compliance.

But help is here. If you follow the steps outlined in the Five-Month Plan below, your organization can be well on its way to being GDPR-ready by May 25, 2018, when GDPR goes into effect across the EU.

What is the GDPR and why does it matter?

The GDPR is part of a wave of new EU privacy legislation that is due to come into force on May 25. Together with other regulations, GDPR looks to radically change the use and flow of personal data worldwide. Importantly, GDPR and the other new rules will apply to all kinds of businesses and a broad range of personally identifiable information.

Aside from the potential for huge monetary fines, an overriding concern 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 likely to take time to implement.

Does it apply to my business?

Assuming that you are a non-European company, you need to ask two key questions to determine whether you need to comply with the GDPR:

1. Do you "process" the personal data of EU data subjects? This is interpreted broadly and can include accessing, storing and transferring personal data of citizens and residents of the EU. In fact, it is difficult to think of anything an organization might do with such data that will *not* fall within this definition. "Personal data" includes data that could identify a person and extends to data that, 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, such as names, email addresses and phone numbers but any data relating to a living person, including online identifiers (IP addresses, device identifiers and Twitter handles), location data and, of course, sensitive data such as medical information – is likely to be considered personal data. Importantly for US companies, this is broader than how PII has come to be defined here.
2. Is your processing of such personal data related to the offering of goods or services to such EU data subjects (no payment is required) or the monitoring of their behavior (i.e., tracking individuals on the internet to analyze or predict their personal preferences)? With respect to number one in the preceding sentence, the mere accessibility of an organization's website from within the EU is not sufficient to meet the requirement that the data is processed "in connection with goods or services." Similarly, the existence of contact addresses for the organization that are accessible from the EU and/or the use of a language used in the EU are also not sufficient. However, the use of an EU language/currency, the ability to place orders in that other language, and references to EU users or customers will be relevant to the determination as to whether the EU data is "processed in connection with goods/services."

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 personal 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:

- **Strengthening rights for individuals**, setting a higher standard for consent (which will affect privacy policies and online data collection processes) and facilitating the ability of people to withdraw their consent and exercise a variety of additional rights.
- **Processor obligations**, imposing on entities that handle data on behalf of others new statutory obligations (in addition to any imposed by contract).
- **EU representative**, requiring some entities based outside the EU to appoint one.
- **Breach notification requirements**, establishing a new duty to report certain types of data breach to the relevant supervisory authority and, in some cases, to the affected individuals.
- **Expanded security requirements**, mandating that systems be designed with privacy in mind and security proportionate to risk.
- **Accountability**, necessity of keeping records of measures used to comply, allowing everything to be documented (e.g., plans, policies and any other materials relating to their handling of personal data).

What happens if I don't comply?

It depends on 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 *the greater of* €20 million or 4% of worldwide annual turnover, as well as imposition of a ban by the EU on processing EU personal data. Or it could result in delaying or losing out on a transaction or investment opportunity because you are not GDPR compliant.

Sounds pretty important, but am I too late?

It is important. The good news is that if you start preparing now, you can be ready for when the new rules go into effect.

Month 1/January 2018 (aka now!): 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 the effort
- Involve management across the organization and engage the board
- Allocate budget
- Commence initial data protection and cybersecurity training

Month 2/February 2018: Information gathering/gap analysis

- Conduct a GDPR information gathering exercise to identify what personal data the company holds or has access to and where, and inventory such information
- Carry out a gap analysis to map data flows against GDPR requirements to identify any weaknesses and failures
- Develop an implementation plan to identify and prioritize risk-based actions

Months 3 – 5/March – May 2018: Implementation

- Review, prepare and update privacy and other relevant policies, external and internal notices, contracts with third parties, internal practices and processes related to data handling, data security and incident response, and record keeping
- Seek out GDPR-compliant technology and develop strategies for "privacy by design" and "privacy by default" so as to minimize processing and retention; use encryption and pseudonymization where possible

Month 5/May 2018 and beyond: Monitor and maintain

- Ensure regular training across the business
- Provide for regular monitoring of updated systems, policies and procedures
- Ensure at least yearly data protection impact assessments

The key takeaway

Each business, large or small, will face its own personal challenges with regard to implementing GDPR. However, adopting a pragmatic, strategic approach, both operationally/technically and legally, will allow you to use the promulgation of GDPR as an opportunity, including allowing other business partners to check the box on your compliance with GDPR.

GDPR compliance will, if properly managed, not only avoid fines and damage to reputation but should also drive

efficiencies and, at the very least, facilitate the ability to leverage and monetize data as the valuable asset that it is.

Sarah Pearce is an expert on data protection and regularly assists clients with privacy and data security compliance and risk management, including most recently assisting clients as they prepare for GDPR compliance.

Randy Sabett, CISSP, is vice chair of Cooley's privacy & data protection practice group. He counsels clients on a wide range of cutting-edge cybersecurity, privacy, IoT, IT licensing and intellectual property issues.

Diane Savage is a member of the technology transactions group. Diane's practice focuses on the legal and business needs of emerging growth companies with primary emphasis in electronics.

Matt Johnson focuses on assisting higher education institutions and education technology companies regarding a variety of regulatory issues including state and federal privacy laws at the K-12 and postsecondary levels.
