GDPR: WHAT IT MEANS FOR US-BASED COMPANIES

schellman
Quality, above all.

OVERVIEW

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was created to best uphold the fundamental personal information rights of individuals and further unify the member states of the EU in their endeavor to manage and protect data. The GDPR's predecessor, the Data Protection Directive (the Directive) was in place to afford similar protections to data subjects. However, since the Directive's adoption in 1995, we've seen tremendous changes to the technology landscape and a constancy of cross-boarder data transfers, and we've recognized that the protections offered through the previous legislation were antiquated and obsolete. With the introduction of the GDPR, individuals have been empowered like never before, and organizations bound to the new framework are starting to feel the weight of that.

HOW IT WILL AFFECT US-BASED COMPANIES

The US stands to be affected directly by the GDPR because the new privacy model applies to any enterprise in the world that targets the European market in offering goods or services or profiles European citizens, and as a result, must process the personal data drawn from those member states. All companies processing EU personal information will have until May 25, 2018 to comply with the reform. Many of the companies that will be affected directly already have existing policies and procedures around privacy due to their need to be compliant with the previous Directive. It is important for these companies to note that the GDPR added new protections for EU data subjects that will require revisions of their current privacy and compliance programs.

DATA BREACH NOTIFICATION

The GDPR's breach notification requirements are far more prescriptive and demanding than the Directive and will likely require most US-based companies to amend their breach notification policies and procedures to comply with the GDPR. In instances where personal data freedoms and rights may be violated, data processors must notify data controllers without undue delay and data controllers must notify the supervisory authority within 72 hours. The documentation and communication of breaches must be delivered in an outlined form and adequately detail certain key information about what's occurred and how it's been handled. When the timing obligations are not met, it seems as though the GDPR has battened down the hatches of the upstream and downstream obligations and it may require organizations to slightly overhaul their data sharing relationships. However, a likely benefit to come from this effort is that companies will be able to simplify their policies and procedures so that they uniformly overarch the expectations of all EU member states and US-based companies will be able to dispatch a single notice.

DATA PROTECTION OFFICER

Under the GDPR, data controllers and processors may designate a data protection officer (DPO) where the main activities of a company involve monitoring of data subjects on a large scale or when the company conducts large-scale processing of special categories of personal data. This new requirement can be met by a company's current privacy or compliance professional. There is still a great deal of uncertainty as to what the role of the DPO will encompass and what the parameters on appointment are. Further guidance is to be issued on the matter that American companies should keep an eye out for.

CONSENT

Under the old Directive, companies were able to rely on implicit and "opt-out" consent in some circumstances. Under GDPR, silence, pre-ticked boxes, or inactivity will no longer constitute consent. Data subjects must confirm choice by a freely given, specific, informed, and unambiguous statement or a clear affirmative action. Like with the Directive, GDPR has distinct requirements for processing special categories of personal data, but has added more to the list. Data subjects must be given the right to withdraw consent at any time. Lastly, the GDPR has introduced restrictions on the ability of children to provide consent without parental authorization.

DATA TRANSFERS ACROSS BORDERS

US-based companies will be able to transfer data to third countries, territory, or a specified sector within a third country, or international organization so long as they have been granted an adequacy designation or appropriate safeguards. Data transfers across boarders are also allowed when appropriate safeguards are in place for a company. US companies should know that the designation or retraction of the adequacy award is binding in all EU member states.

RIGHT TO BE FORGOTTEN AND DATA PORTABILITY

The GDPR introduced two new rights for data subjects. The right to be forgotten was codified to allow individuals to request the deletion of their personal data. The GDPR also gives the data subjects the right to receive data in a common format and to have their data transferred to another controller if the data subject so requests.

VENDOR MANAGEMENT

Under the GDPR, the controller is liable for the actions of the processors they choose. It is important that US-based companies carefully choose their processors. A relationship between a controller and a processor should be governed by a contract. The contractual relationship should include details around the data itself, retention periods, disposal requirements, the nature and purpose of the data, etc...

PSEUDONYMIZATION AND ANONYMISATION

Under the GDPR, personal data does not include data that does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable. US companies who are familiar with HIPAA may be familiar with this concept given it's similarities with de-identification of protected health information. The GDPR plainly endorses the use of pseudonymization and there are incentives for companies who choose to apply it to the data that they collect. US-based companies should explore this method as an option if it is not something they currently do with the personal data they collect and/or process.

CODE OF CONDUCT AND CERTIFICATIONS

Due to the difficult task of ensuring that each company is compliant with the GDPR, codes of conduct and certifications have been endorsed as guidance to the requirements and as proof of compliance. US-based companies should familiarize themselves with the differences in each to ensure they choose the best one for their business model.

ENFORCEMENT AND FINES

The new enforcement procedures and fines associated with the GDPR are perhaps what have most companies nervous about. The hefty fines associated with the non-compliance of the GDPR can reach the millions or even billions of dollars. Violators will be placed in one of two tiers, with the higher tier costing violators up to over 20 million euros or 4% of the company's net income.

CONCLUSION

The GDPR has revealed itself to be the highest denominator in privacy doctrine in history. It's greatly broadened its definition of personal data and overhauled or bolted on principles that will take some time for organizations to tackle, even if privacy-mature and familiar with the Directive. May 25, 2018 may seem like an eternity away as we only near the end of 2017, but be assured that the GDPR was intentionally designed with a long fuse given the necessary reform it involves. Albeit challenging maybe for US-based companies in certain respects, the GDPR must be hailed as an awesome step in the direction of promoting the rights of natural persons and should ultimately strengthen global relations and commerce.

GETTING STARTED

- Familiarize yourself with the chapters and articles in the GDPR program. Schellman has additional content beyond this white paper shared through blogs and recorded webinars.
- Understand how and where your organization ingests, stores, and transfers European personal data.
- Assess how privacy mature (or immature) your enterprise is.

CONTACT US TODAY

Schellman offers several competitive differentiators for organizaions looking to align themselves with the GDPR. We are the first CPA firm that is 100% independent with no consulting agenda. We also offer organizations the opportunity to consult with our distinguished subject matter experts:

Avani Desai
Executive Vice President
CISSP, CISA, CIPP, CCSK

For more information or to contact us about your GDPR initiatives, go to www.schellmanco.com/gdpr


schellman