ABA Section of International Law
Your Gateway to International Practice
Volume 6, Issue 2
Winter 2017

Privacy, Cybersecurity & Digital Rights Committee
Quarterly Newsletter

**Impacting your Company … in just a few months**

**… GDPR!**

By Aaron Schildhaus, Counsel, Scharf Banks Marmor LLC

If your company has, or is contemplating, any business activities or relationships in the European Union (EU), you will be affected by the EU's General Data Protection Regulation (GDPR), even if your contacts there are minimal. The GDPR comes into full force and effect May 25, 2018, and companies around the world are preparing for it. Failure to be in compliance with this new law will put companies at risk for enormous fines and penalties: up to the greater of 4% of annual global revenues or €20 Million for data controllers and, for data processors, up to the greater of 2% of annual global revenues or €10 Million.

The GDPR is replacing the existing Data Protection Directive 95/46/EC, which has been the standard for data protection and data privacy in the EU since it came into force in December 1995. US companies now in compliance with the directive, including the 2400 companies which have qualified for the EU-US Data Privacy Shield, and its analogue, the Switzerland-US Privacy Shield, should be aware that compliance with the current data protection regime will not be sufficient, in and of itself, to qualify under the GDPR.

The GDPR was designed to deal with the growing need to further protect the European individual from being compromised by the misuse of personal data in the possession of organizations; it sets to harmonize privacy and data security laws across Europe and to reshape the way organizations across the region approach data protection. Because the GDPR is a regulation, and not a directive, it will be directly applicable in all EU Member States. It should be noted that the UK's upgrading of its Data Protection Act with the Data Protection Bill essentially conforms to the GDPR so that its businesses can remain competitive with the EU despite Brexit. In any event, the UK's exit from the EU will not take place before the GDPR takes effect in May; therefore, UK businesses will be subject to the GDPR, too.

Article 1 of the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data … (and it) … protects fundamental rights and freedoms of natural persons and in particular their right to the protec1ti on of personal data."

The GDPR and its implementation will have a profound effect on data protection and privacy not only in Europe, but worldwide, given the trans-border realities of electronic data management and processing and the regulation's new, extra-territorial provisions. It applies to all companies, regardless of location, that process the personal data of data subjects residing in the EU. The GDPR also applies to the processing of personal data of data subjects in the EU by controllers and processors in the EU, wherever the processing takes place, whether or not in the EU.

Another extra-territorial provision of the GDPR is that it applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to the offering of goods or services to EU citizens (whether or not payment is required) and the monitoring of behavior that takes place within the EU. Previously, under the directive, territorial applicability was ambiguous, referring to data processing in the context of an establishment. The extra-territoriality of the Regulation is now clear; moreover, non-EU businesses processing the data of EU citizens will have to appoint a representative in the EU.

In addition to its application outside of Europe and the potentially high penalties for its violation, other notable changes in the GDPR over the current data protection regime include:

- A request for the data subject's consent must be given in a concise, transparent, intelligible and easily accessible form, and the consent must be given for one or more specific purposes.
- The right to erasure (right to be forgotten). Set forth in Article 17, it entitles the data subject to have the data controller erase his/her personal data, cease its further dissemination, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing, or data subjects withdrawing their consent. When considering such requests, controllers are required to compare the subjects' rights to "the public interest in the availability of the data."
- The right for rectification set forth in Article 16.
- The right of data subjects to obtain free reports re type and purpose of data, names of data processors;
- The requirement that companies of a certain size have their own internal Data Protection Officers (DPO's);
- Establishment of DPO criteria;
- The requirement that forms providing for data subject consent be clear, concise and intelligible;
- The requirement that it be as easy to withdraw consent as to grant it;
- Mandatory breach notification within 72 hours where a breach risks individual rights and freedoms;
- Data portability by data subject; right to transmit data to another controller;
- Privacy by design; advance determination of minimum information required by controller.

If a data breach occurs, notification must be given within 72 hours from first awareness of the breach in all member states where said breach is likely to "result in a risk for the rights and freedoms of

individuals". Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Data protection by design under the GDPR means that data protection must be a consideration from the onset of the designing of systems, rather than an addition. 'The controller shall implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation.in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

Under the GDPR it will not be necessary as is currently the case, for data processors to submit notifications / registrations to each local Data Processing Authority (DPA) of data processing activities, nor will it be a requirement to notify or obtain approval for transfers based on the SCCs). Instead, there will be internal record keeping requirements, and the DPO's appointment will be obligatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or of special categories of data or data relating to criminal convictions and offences. The DPO must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices, and may be a staff member or an external service provider. The DPO's contact details must be provided to the relevant DPA. In addition, the DPO must be provided with appropriate resources to carry out its tasks and maintain his/her expert knowledge. The DPO must report directly to the highest level of management, and must not carry out any other tasks that could result in a conflict of interest.

Compliance possibilities by entities continue to include the use of Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCC).

***

**Aaron Schildhaus** is Counsel to Scharf, Banks & Marmor, PC, a Chicago law firm, specializing in corporate litigation and transactions. His practice is focused on US – EU data protection and privacy compliance, FCPA compliance and due diligence, and international transactions involving the US, Europe, Africa, India, the Middle East and Latin America, representing NGO's and large and small corporations in the US and abroad. He is past Chair of the ABA Section of International Law and has spoken frequently internationally, and written numerous articles, on data protection in Europe and on a wide variety of other business related legal topics**.**