Fisher Broyles

June/July 2018

Corporate Law Update

The EU's General Data Protection Regulation: Why It Matters to You

The European Union has traditionally been more protective of privacy than the United States, which has led to substantial challenges for many US companies. Those challenges are now greater and affect many more US businesses as a result of the recent EU adoption of the General Data Protection Regulation (GDPR), which represents a sea change compared to prior law. Rather than a mere rule or two, the GDPR is a complicated set of myriad requirements. Frequently, a major misconception is that GDPR requires only an update to a company's privacy policy and compliance with such new policy, but as noted below, there are numerous other provisions which are equally important. We also anticipate companies being required to make representations and warranties regarding GDPR matters in M&A and finance transactions. While a detailed analysis is beyond the scope of this newsletter, the following can serve as an introduction to some key provisions.

Expanded Territorial Scope

GDPR has a much broader territorial scope than prior EU law. It applies to the processing of data by companies with an EU "establishment". The term "establishment" is not precisely defined, but some consider it to mean regular activity in the EU and/or consistent interaction with EU citizens. Accordingly, the GDPR applies to any individual or business that collects or processes personal data of any EU individual or monitors the activities of EU residents, notwithstanding the lack of physical presence in the EU. As a result, many US companies with no physical presence in the EU are now subject to GDPR based on customers or other business contacts with EU residents. Companies that do not have an establishment in the EU but that are subject to GDPR are also required in many cases to appoint a personal representative in the EU, which will in effect make the company subject to EU jurisdiction despite the absence of an EU presence. However, it is always essential to determine if a company is in fact obtaining any personal information from anyone in the EU or have taken steps to avoid doing so.

Data Mapping

In order to determine required steps for compliance, it is essential to "map" one's data. This means determining what data is being collected, from whom and where it is going for storage, processing or otherwise, and then creating and maintaining a written record of the foregoing.

Consent and Other Requirements

One of the many huge changes from prior EU law is found in the area of consent to collection and use of personal data. In most cases GDPR now requires recorded affirmative consent to the collection, use, and storage of personal information of an EU resident; opt-outs are not sufficient. The request for consent must meet a number of strict requirements, including that the request: (i) be presented in plain, clear language; (ii) include the purposes for collecting and processing the data; and (iii) be freely given, specific, informed and unambiguous. GDPR further requires that data subjects have a broad set of rights, including access to their data, rectification of any incorrect personal data, erasure of personal data (also known as the "right to be forgotten"), and data portability.

Data Transfers

Under GDPR, transfers of personal data from the EU to the US may occur only if special frameworks are in place to guarantee "essentially equivalent" protection of the data. These include, among other things, adopting EU-approved Standard Contractual Clauses and enacting Binding Corporate Rules for intra-company transfers. Such transfers often require the presence of agreements with counterparties to govern security and usage. Such agreements will often involve companies asking each other to acknowledge that they are "data processors" or "data controllers." Being a data processor or data controller entails significant legal obligations, so undertaking such roles should only be done after careful consideration.

Data Protection Officers

Many organizations must now formally designate a qualified Data Protection Officer (DPO) who is responsible for the organization's efforts, and other organizations may find it advisable to do so even if not required. The DPO must be vested with appropriate authority to implement applicable requirements, possess pertinent knowledge and training, and have no other duties that could create a conflict of interest with his or her data protection duties for the company.

Compliance and Enforcement

The above is only an introduction and a partial list of the new requirements. GDPR will clearly impose substantial new burdens on many companies and potentially alter how they do business. GDPR was published in 2016, giving companies two years to prepare, and now EU regulators are poised to begin enforcement. Compliance is crucial given that potential penalties are as much as the greater of twenty million Euros or four percent of worldwide annual revenue.

Our Privacy and Corporate partners are pleased to work with you to discuss all GDPR issues.

Contacts

If you would like additional information, please contact any of the following FisherBroyles partners:

Atlanta
Carl Johnston
carl.johnston@fisherbroyles.com
(404) 330-8179

Chicago
Marty Robins
martin.robins@fisherbroyles.com
(847) 277-2580

Los Ageles
Steve Papkin
steven.papkin@fisherbroyles.com
(310) 415-6254