Subscribe To Data Privacy Law

Email Address *

SUBSCRIBE!

Search Posts

Categories

- Webinars & Podcasts
- Jaffe Updates
- News
- Electronic Payments Law +
- Michigan Green Law +
- Data Privacy Law +
- Immigration Law +

Download PDF

FEBRUARY 3, 2017 | JON SRIRO

The GDPR and the Model Clauses for Data Transfer Processors: Transactional and Litigation Issues

Whether we like it or not, whether we adopt similar legislation in the U.S. or not, the stringent requirements of the General Data Protection Regulations ("GDPR") are coming and the requirements are becoming a boilerplate language in U.S. contracts. This will impact businesses as it relates to their operations, contract negotiations and, eventually, exposure to liability. As a result, attorneys will need to become well versed in the GDPR.

There are several reasons for the operational and legal influence of the GDPR in the U.S. These reasons, among other things, include the following:

- Companies that do business in the EU are starting to gear up for the compliance requirements when the GDPR goes into effect on May 2018. As a result, companies are now demanding compliance for all vendors with which they share data; this requires operational changes and updated terms for contracts.
- Companies are receiving demands for stricter data protection, so they are passing on these requirements to domestic vendors that have access to their data or their customers' data, even though the transaction does not by itself trigger EU jurisdiction.
- Companies are learning more about data protection issues and are adopting contractual requirements that are more protective of their data and their customer's data. Many of these companies are using the EU model contract clauses ("Model Clauses") as a starting point.

In order to understand the requirements placed on parties sending and receiving data, it is important to understand some basic terms that the GDPR relies upon for delegating responsibilities and liabilities. A "data processor" is generally the entity which processes personal data on behalf of the data controller. U.S. companies that receive data from the EU would, in most cases, be considered a "data processor" or a "data importer." On the other hand, a "data controller", or "data exporter" is generally the entity which transfers the data to the data processor and instructs the data processor what to do with the data.

The requirements of the Model Clauses are reasonable from the perspective of the owner of the data, but the requirements may be difficult for most U.S. companies to agree to. Most U.S. companies have not invested the time or money for this level of compliance or data protection. Further, any U.S. company that agrees to this language is exposing itself to tremendous liability to data subjects/end users.

The EU, through the GDPR, seeks to impose its jurisdiction over data processors in foreign countries that are not members of the EU. The GDPR provides rules for any data processor that processes personal data from the EU, regardless of whether the processor is located in the EU. According to the GDPR, data processors will be subject to the jurisdiction of the data subject's member state, regardless of where the data processor is located. It is unclear how the U.S. courts will react to the jurisdiction that the EU seeks to impose on data processors in the U.S.

Under the GDPR, data processors will also be subject to significant fines and sanctions. Data processors that agree to the Model Clauses will have direct obligations and liability to data subjects, i.e., third-party liability. Data subjects will be able to pursue claims against data processors, despite there being no privity of contract or required third-party beneficiary designation.

Some areas that may trigger liability for data processors under the GDPR include the following:

- Failure of the data processors to implement appropriate technical and organizational safeguards to ensure processing meets the requirements of the GDPR;
- Failure of the data processor to process personal data in accordance with the controller's instructions;
- Failure of data processors to get written consent to subcontract work to a third-party that will be processing data (a sub-processor);
- Failure of the sub-contractor to comply with all of the data processors' obligations related to the data it handles;
- Failure to maintain adequate records demonstrating compliance;
- Failure to notify the data controller of a breach without undue delay; or
- The list goes on and on…

In addition, the GDPR imposes significant sanctions for the failure of a data processor to comply with its requirements. Sanctions include up to 4% of a data processor's annual global turnover for certain breaches. It is not clear if limitations of liability in a company's terms of use for data subjects or in its contract with the data controller will be a basis to limit the sanctions.

Although there may be components of the GDPR and its Model Clauses that are not adopted by the U.S. or that are not deemed enforceable against U.S. companies by the courts, it is clear that through legislation or practice, some of the stringent GDPR requirements will be adopted in the U.S. for the handling of sensitive and personally identifiable data.