NEWMEYER & DILLION LLP

Does Your U.S. Company Pull Data From European Citizens? Fall In Line with GDPR by May 2018 or Suffer Substantial Fines

By: Jeff Dennis & Ivo Daniele

Jeff Dennis

Contact

949.271.7316

Email: jeff.dennis@ndlf.com

Practice Specialties

Business Litigation
Construction Litigation
Cybersecurity
Insurance Law
Real Estate Litigation

Ivo Daniele

Contact

925.988.3222

Email: ivo.daniele@ndlf.com

Practice Specialties

Business Litigation
Construction Litigation
Cybersecurity

The European Union ("EU") has enacted a strict, comprehensive framework of security regulations aimed to protect its citizens. These regulations, known as the General Data Protection Regulation ("GDPR"), provide a blueprint for a combination of required legal, technological and work habits within an organization. Although this is an EU regulation, the new laws will apply to any organization within or outside the EU that collects or processes data of EU citizens. Therefore, U.S. companies must analyze their data and processes to determine whether compliance with the GDPR is necessary. A quickly-approaching deadline of May 25, 2018 must be met to avoid massive fines.

What is the GDPR?

In order to address the creation of social networking sites, cloud computing, and location-based services, the EU set in motion a process to implement a vigorous set of rules to ensure the right to personal data protection for all European citizens. In April 2016 the European Parliament, the Council, and the Commission adopted a new GDPR, which will take affect on May 25, 2018.

This GDPR will streamline cooperation between the data protection authorities on personal data issues allowing companies to deal with one authority - not each of the 28 EU member states. This will allow for quicker decisions by the data protection authorities and greatly reduce the red tape in both compliance and enforcement under the GDPR. This will also create a level playing field by forcing non-EU companies to comply with the same strict regulations - regardless of whether or not the company is established in the EU.

Territorial scope of the GDPR

The GDPR applies directly to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU - regardless of whether the processing takes place in the EU. Additionally, there are specific provisions under the GDPR that apply to non-EU companies if their processing activities relate to (a) the offering of goods or services (irrespective of whether a payment of the data subject is required) or (b) monitoring the behavior of individuals within the EU. Therefore, all companies must determine whether they process or monitor information of EU citizens. If a company falls within one of these categories, compliance with the GDPR is mandatory.

What happens if a company fails to comply with the GDPR?

Failure to comply with the GDPR could subject a company to crushing administrative fines.

The supervisory authority has the power to impose administrative fines under the GDPR. The following violations and breaches would subject a company to administrative fines:

- Not adhering to the core principles of processing personal data,
- Breach of notification to EU citizens by controllers and processors,
- Wrongful transfer of personal data to non-EU countries,
- Breach of obligations regarding certification,
- Ignoring the mandates asserted by the supervisory authority,
- Breach by those responsible for impact assessment, and
- Wrongful processing of employee data.

The extent of the violation and type of personal data involved will dictate the severity of the administrative fines imposed on a company. For example, under the GDPR, a company could be subject to administrative fines up to 20,000,000 EUR, or up to 4% of the total worldwide annual revenue of the preceding financial year. Obviously, these fines would be financially crippling to any company.

Preparing for May 25, 2018

The May 25, 2018 deadline is fast approaching and preparing for full compliance with the GDPR is paramount. Simple steps should be taken to ensure compliance including to:

1. Review and analyze data repositories for sensitive data,
2. Perform an analysis/accounting of procedure for data collection, and
3. Create an oversite committee dedicated to data activities and compliance.

Most importantly, however, is to determine whether compliance with the GDPR is necessary, and strictly follow the requirements of the GDPR to protect from potentially massive fines.

Jeffrey M. Dennis currently serves as Newmeyer & Dillion's Managing Partner and as a business leader, advises his clients on cybersecurity related issues, introducing contractual and insurance opportunities to lessen their risk. You can reach Jeff at jeff.dennis@ndlf.com.

Ivo Daniele is a seasoned associate in Newmeyer & Dillion's Walnut Creek office. His practice includes representing private and public companies with both their transactional and litigation needs. You can reach Ivo at ivo.daniele@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.