Beware of the New General Data Protection Regulation: Is Your Business Collecting Personal Data from EU Citizens?

Amundsen Davis Corporate Alert
June 22, 2018

The new General Data Protection Regulation (GDPR), which came into effect May 25, 2018, arguably applies to all companies that collect and process data belonging to European Union (EU) citizens. The GDPR claims extraterritorial reach that applies to U.S. companies. Article 3 of the GDPR states that the regulation applies to any data processor established in the EU and any data processor not located in the EU if the data being processed relates to offering goods and services to data subjects in the EU or monitoring their behavior that takes place in the EU. Some U.S. companies are scrambling to come into compliance with the new implementation of the GDPR. U.S. companies have good reason to comply because failure to comply could be costly. The fine for non-compliance can be up to 4% of global annual turnover or 20 million euros, whichever is greater. For many companies, a fine of this size could be devastating.

The GDPR requires companies to review and implement changes to their existing policies regarding data processing, storage, and collection. One of the main new provisions in the GDPR which sets it apart from prior data protection policies is that the data processor must get a data subject's consent to process, store, and collect the data subject's personal data. Article 7 of the GDPR lays out the conditions for consent that must be met for a data processor to process personal data of a data subject. The request for the data subject's consent must be in a clear and plain language if in the written context. The data subject must also be able to withdraw his or her consent at any time and it needs to be easy for the data subject to do. Finally, under Recital 32 of the GDPR, consent must be an affirmative act rather than passive acquiescence. Companies should not deem silence, pre-clicked boxes, or inactivity as consent as this is not enough under the GDPR. However, having the data subject click a box, is fine for consent. The new regulation makes consent a top priority.

RELATED SERVICES

Corporate & Securities

Cybersecurity & Data Privacy

AMUNDSEN DAVIS

The GDPR has strengthened many rights of the data subjects relating to their personal data. The data processor must now notify the supervisory authority of a data breach to its system within 72 hours of the data breach, under Article 33 of the GDPR. If the supervisory authority is not notified within 72 hours, the data processor must inform the authority of the reason for the delay. At a minimum, the notification of the data breach should describe the nature of the data breach, identify a point of contact where more information can be acquired, describe the consequences of the breach, and describe the actions taken to mitigate the effects of the breach. The data processor should then document the breach and keep that information, as the documentation will enable the supervisory authority to validate compliance with Article 33.

The GDPR also now gives data subjects the right to access their personal data and the "right to be forgotten." Article 15 of the GDPR gives data subjects the right to access their personal data. The data subject is entitled to obtain from the data processor information such as the purpose of the processing, the third parties who may receive their personal data, the period of time for which the data will be stored, the existence of the right to request the personal data be corrected or deleted, and the right to lodge a complaint. In addition, the data subject must be provided a copy of their personal data upon request. If the data subject requests the data processor to erase its information, the data processor must comply without undue delay. This right is found in Article 17 of the GDPR.

With this new, far-reaching regulation, U.S. companies should work with their general counsel, or outside counsel, to ensure they are in compliance with the GDPR if they process data on subject in the EU. In addition, U.S. companies can use the EU-U.S. Privacy Shield Framework from the U.S. Department of Commerce to certify compliance with the GDPR. At the very least, U.S. companies should review their existing privacy policies and make any necessary amendments. As time goes on, there will be more guidance on the GDPR, so U.S. companies should keep an eye out for updates and advice on the GDPR. A best practice for any company is to have a data breach response plan in place and to identify a Privacy Officer.