CLIENT ALERTS & INSIGHTS

EU Data Protection Law Subjects U.S.-Based Companies to Potentially Substantial Penalties

FEBRUARY 3, 2017

Authors: Michael D. Stovsky

On May 25, 2018 the European Union's General Data Protection Regulation and Regulation (GDPR) on Privacy and Electronic Communications (the "ePR") will go into full force and effect. That gives companies that do business in the EU, or collect data from residents of EU nations, only a short period of time to comply fully with these very strict new rules.

The EU General Data Protection Regulation [1]

Though the GDPR does not take effect until May 25, 2018, company's should take steps now to consider how the GDPR will affect its business, whether compliance is necessary, and if so, to implement a program to ensure compliance by the effective date.

The GDPR applies to all organizations that collect, process, or transfer personal data of individuals located in the EU. Therefore, any company in the world that that offers goods or services to individuals in the EU, whether payment is required or not, must comply with the regulation. "Personal data" is defined very broadly and includes a wide variety of information relating to an individual including their name, photo, email address, bank account information, posts on social networking websites, medical information, geo-location data, and their computer's IP address.

The fines for violations of the GDPR regarding data processing can be up to the greater of 20 million euros or 4 percent of the annual worldwide turnover of the preceding financial year of the violator (an amount which essentially equates to the gross revenue of the violator).

The GDPR implements certain obligations in response to a security breach. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal information requires that the controller of the data notify the designated data protection authority "without undue delay" and not later than 72 hours after becoming aware of the event. If the breach creates a "high risk" to the rights of individuals, the affected data subjects must also be notified without undue delay.

Another complication for U.S.-based companies is that the GDPR implements new requirements for organizations to obtain consent from data subjects prior to collecting personal information. Consent must be obtained through affirmative conduct and the data subject must be properly informed of the uses of their personal information. Furthermore, the data subject must also have the ability to revoke consent at any time without detriment.

Regulation on Privacy and Electronic Communications

To complement the GDPR, last week the EU published its new ePR. The ePR aligns the rules that apply to the confidentiality of electronic communications with the GDPR. All entities, wherever located, that provide electronic communications services to users in the EU are subject the requirements of the ePR.

The obligations applicable to traditional electronic communications networks and services now also apply to web-based e-mail services. The ePR also contains rules regarding the installation and use of cookies and similar apps, including third party analytics platforms, as well as the sending of unsolicited communications.

Violations of the ePR can lead to penalties similar to the penalties set forth in the GDPR.

Recommendations

We recommend that companies immediately take steps to assess whether any of their activities, products, or services fall within the scope of the GDPR and/or ePR and, if so, to begin the process of becoming GDPR and ePR compliant prior to the May 25, 2018 effective date for these two new and very important regulations.

For further information, please contact Michael D. Stovsky, Partner, Benesch, Friedlander, Coplan & Aronoff LLP, 200 Public Square, Suite 2300, Cleveland, Ohio 44115, (216) 363-4626 or mstovsky@beneschlaw.com.

---

[1] This Alert only provides basic background information regarding the GDPR and ePR. It is not meant to be a full and complete recitation of all of the requirements of the GDPR or ePR and is not and should not be interpreted as legal advice or a legal opinion. This Alert does not create an Attorney-Client relationship. An Attorney-Client relationship will only be established by the execution by Benesch, Friedlander, Coplan & Aronoff LLP and a prospective client of a final engagement letter with respect thereto.