Bloomberg Law

Privacy and Security Law Report®

GDPR

Compliance with the new European Union privacy regime is likely to affect the bottom line of U.S. companies which process substantial amounts of data from EU residents, and the authors recommend that companies begin acquiring an in-depth understanding of the new GDPR requirements now in order to rethink their business, advertising and product design strategies to minimize the GDPR's blow to the bottom line.

The GDPR and the Bottom Line: How the EU Data Privacy Regulation Will Affect U.S. Companies' Data Collection and Processing Practices—and Their Revenue

BY LAURA JEHL AND LISA MAYS

For U.S. companies which do business in Europe or who process the personal data of European Union residents, the world of data privacy and security is about to get much more complicated. While U.S. privacy law is unsettled, with rapidly proliferating state and federal laws and regulations and uncertainty as to how strictly they will be enforced, the rules in the European Union are tough and about to get much tougher. The General Data Protection Regulation (EU) 2016/679 (GDPR), slated to take effect in May 2018, will give consumers in the EU substantially more control over how their personal data is used. The increased control includes the right to:

1. access any personal data that has been collected;
2. obtain confirmation about whether an individual's data is being processed; and
3. require that the data be ''erased'' if the consumer withdraws consent.

Laura E. Jehl is co-leader of the Privacy and Cybersecurity practice at Sheppard Mullin Richter & Hampton LLP in Washington.
Lisa C. Mays is an associate in the firm's Government Contracts, Investigations & International Trade practice in Washington.

Compliance with the GDPR is likely to affect the bottom line of U.S. companies who process substantial amounts of data from EU residents, and not only because of the costs associated with GDPR-mandated data inventories, privacy assessments, data breach notification, and documentation. GDPR's strict rules regarding consent to process personal data—which will require separate ''opt-in'' consent for each processing activity, and the destruction of data after the specific activity is completed—will mean that companies collecting data from EU residents can no longer rely on a consumer's agreement to a broad privacy policy that allows processing of data for purposes that go beyond the provision of the specific service in question. As a practical matter, compliance with these rules will almost inevitably mean that businesses will be able to collect and use far less customer data than they have been accustomed to collecting. For that reason, compliance is likely to affect the revenue that many companies have grown accustomed to generating by using and/or selling their customers' data.

Who Needs to Comply With the GDPR The new regulation will apply to companies that collect or process the personal data of EU residents, transfer data out of the

EU, or target clients in the EU. Companies that handle sensitive data are subject to heightened requirements. The GDPR may affect even companies with no physical presence in Europe, especially those companies that conduct e-commerce or make use of cloud-based services. Moreover, the GDPR covers the provision of free services as well as commercial services. The GDPR will thus affect businesses across a broad range of industries, including hospitality, retail, telecommunications, and any business with employees in the EU.

Perhaps the biggest potential threat to revenue in the General Data Protection Regulation involves the level of consent required of consumers.

When Companies Need to Comply With the GDPR The GDPR enters into force May 25, 2018, but affected companies should be preparing now because the regulations will require significant changes in how customer data are collected, used, and stored. Not only must all systems be ready to go by May 2018, but new and existing contracts whose terms extend beyond the GDPR's effective date will need to include representations of compliance with GDPR. A company's inability today to assure its partners of such compliance in 2018 may put its revenue-generating contracts at risk.

The GDPR's Changes to Consumer Consent Requirements Will Impact Data Collection Practices—and Likely Revenue Derived From Data While the GDPR includes a number of provisions that will require significant changes to present business practices, perhaps the biggest potential threat to revenue involves the level of consent required of consumers. This threat is amplified by the contrast between U.S. and European consumers' approach to privacy. American consumers have shown themselves to be generally comfortable sharing personal information in order to gain access to new products and services, while European consumers have tended to view the privacy of their personal data as a fundamental right and to limit their disclosures accordingly. In order to minimize the impact of compliance on revenue, businesses will need to contend with this cultural divide.

The new GDPR framework mandates that:

1. Consumers must consent to the specific use of their data for each separate processing activity. The consent terms cannot be bundled or included with other agreement terms. Further, after the specific processing activity has been completed, the data must be destroyed. *See* GDPR Art. 7(1), 7(2), 7(4), 17.

2. Consumers may revoke their consent at any time. Such revocation is effective immediately. *See* GDPR Art 7(3).

These new consent requirements will not only create a minefield of operational and compliance issues, but are almost guaranteed to result in companies having access to far less data than they have been accustomed to gathering under the broad, opt-out privacy policies in widespread use in the recent ''Big Data'' years.

Companies that currently gather all consumers' data in the same manner, regardless of their country of origin, will either have to segregate EU from non-EU consumer data or subject all data to the far-stricter treatment required by the GDPR. Treating all data the same would likely save costs associated with changing data flows and systems architecture and would simplify administrative compliance. The cost of such simplification, however, will be measured in greatly reduced data collection.

GDPR's strict opt-in rule will mean that less data is gathered at the outset, as many consumers faced with a clear description of how their data will be used will simply choose not to share it. Moreover, the requirement that data only be used for the specific purpose for which it was initially gathered will mean that consumers must be asked again and again, each time a company wants to use their data. Such repeated requests are bound to cause abrasion, especially for U.S. consumers, further draining the pool of consumers who are willing to consent to use of their data. Since consent may be revoked at any time, companies will also have to develop effective processes for removing consumer data, and may be less likely to process significant amounts of data given the risk of significant fines for inadequate or failed removal. Taken together, these consent requirements will force a sea change in the amount of EU consumer data collected and the frequency with which it is processed.

For many U.S. companies accustomed to gorging themselves on the business opportunities presented by ''Big Data'' gathered under broad, often unread, opt-out privacy policies, implementing GDPR-compliant practices across all their global data collection activities will be almost unthinkable. The opportunities presented by broad data collection—from targeted advertising to customized product development to redesign of stores and restaurants for maximum customer appeal—as well as the revenue that can be generated from the sale of such data have been highly lucrative, and have fundamentally changed the nature of many companies' business operations.

Many U.S. companies will likely choose to segregate their European Union and U.S. data operations rather than implement a one-size-fits-all data policy.

As more and more U.S. companies—from coffee vendors to automobile manufacturers and everyone in between—turn to mobile apps to sell their products and provide marketing to their customers, they are finding themselves effectively transformed into ''data'' companies, reliant on consumers' willingness to disclose personal information and the ability to use that information with few restrictions. This explosion of mobile-app driven commerce, which some in Europe may see as another manifestation of the creeping Americanization of society driven by technology, is a key reason that the new GDPR regulations will be especially challenging for U.S. companies to implement. The underlying concept of mobile-app commerce runs counter to the purposes of the GDPR.

  PVLR ISSN 1538-3423

Thus, many U.S. companies will likely choose to segregate their EU and U.S. data operations rather than implement a one-size-fits-all data policy. This will increase costs of systems architecture and data transfer changes, require two sets of staff or at least two sets of guidance on how to respond to customer requests and complaints, and result in the loss of value and insight currently obtained from EU customers. Unless the U.S. cracks down on privacy along a similar opt-in model—a prospect that is not currently on the horizon—the GDPR will likely cause a widening of the gulf between the business practices—and potential innovation—of companies with regard to data collected from U.S. and EU consumers.

Enforcement of the GDPR While it remains unclear how strictly the GDPR will be enforced, the GDPR grants the national data protection agencies greater enforcement capabilities than they currently possess. These include the ability to impose financial penalties for breaches of data privacy, up to a maximum fine of 4 percent of global annual turnover, or 20 million Euros ($22.3 million), whichever is greater.

In addition, agencies will be able to detect violations by simply checking a company's posted privacy policy to determine whether it is GDPR-compliant. The low level of enforcement cost will most likely enable agencies to identify and prosecute a higher volume of potential violations.

For these reasons, we recommend that companies begin acquiring an in-depth understanding of the new GDPR requirements now in order to rethink their business, advertising and product design strategies—as well as to implement required compliance procedures—to minimize the GDPR's blow to the bottom line.