Securities
Regulation Daily

Wolters Kluwer

December 18, 2017

Why and How Europe's New General Data Protection Regulation Impacts US Companies

By Cynthia J. Cole and Neil Coulson, Baker Botts LLP*

In the first of a series of two articles, Baker Botts' attorneys Cynthia J. Cole and Neil Coulson set out why Europe's new General Data Protection Regulation will impact domestic businesses. In Part 2, they will provide practical guidance to businesses on steps they can take to ensure compliance.

Data privacy experts see a troubling trend among American companies that collect, store and analyze personal data: there is a lack of knowledge about how Europe's General Data Protection Regulation ("GDPR") will affect them.

Few US companies are making the big changes required to comply with this new law and many do not realize how GDPR may affect them and what happens if they are not compliant. GDPR goes into effect on May 25, 2018, and, to the surprise of many American corporations, it will dramatically impact how they handle the personal data of their customers.

GDRP's reach extends far beyond the boundaries of the EU. American and international companies, no matter where they are incorporated or where their physical facilities are located, will be required to comply if they touch the personal data of people living in Europe. If they touch that personal data in connection with the offering of goods or services in the EU, or they monitor the behavior of EU residents, GDPR affects them.

GDPR upends the traditional approach to customer data collection. Until now, companies have regarded data as an asset to be captured, analyzed and utilized for marketing. Data is king, and companies who excelled at using it have profited greatly. GDPR changes the stakes.

The risk of noncompliance could be severe. Companies found in violation of this new rule, regardless of their location, could be subject to fines equaling 4% of annual turnover or €20M (**almost $24M**), whichever is higher.

How Are American Companies Affected by GDPR?

Under GDPR, anyone living in Europe who goes online and enters their name, email address, photo or any information through which they can be identified onto a website will be protected by GDPR.

---

* Baker Botts partner **Neil Coulson** is the Department Chair - Intellectual Property in London and Moscow. **Cynthia J. Cole** is Special Counsel in Palo Alto in Baker Botts' corporate, technology and privacy and data security practice groups.

If anyone is purchasing online and entering their bank account or credit card information, or if the website just captures their IP addresses, that falls under the protection of GDPR. A company requesting an email address for their mailing lists, a credit card number to pay for a purchase, or even the recording of an IP address to target appropriate online ads, must now must comply with GDPR.

GDPR applies to personal information whatever the company is selling. It is irrelevant if the information is obtained and held by the seller itself, by a payment processor or in the cloud. If a consumer's data is held and used for the company's commercial purposes, it must be done with the **express consent** of the customer and for a legally permissible purpose to the benefit of the consumer.

Why the Change?

GDPR was passed to "harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy."

The law holds that data collection "must serve a specified and legitimate purpose, and data must be used only in ways deemed necessary for that purpose. The data may only be stored for as long as is necessary to meet that purpose, and must be protected with appropriate security. "

GDPR requires companies that hold personal data like email addresses, banking information and IP addresses "to demonstrate that their procedures comply with these principles." Compliance must be shown by a legally permissible rationale for data collection and processing (*i.e.*, the information is necessary for the performance of the contract, or the company needs your address to send you the product or your credit card information to process payment) and documented consent by the consumer.

What should US Companies Do?

Philosophical Change

Companies operating within the framework of GDPR must change the way they use their customers' information. Businesses need to build concepts of privacy into their operations model and run constant privacy impact assessments. Companies must develop new policies respecting an individual's data rights over the rights of the company.

Businesses who hold the personal data of EU residents will have to provide demonstrable proof that at every step of the information chain they are safeguarding that data.

This includes asking for consent to use that information at every step in the process. Companies must inform the customer about all that they are doing with their personal data, and why it is being used.

Procedural Changes

- Companies who engage in large scale collecting, processing or monitoring of data including online tracking and profiling of people's behavior for advertising, should hire or appoint a Data Protection Officer to enforce compliance.

- Terms and conditions and privacy policies must be accessible, reviewed and revised continuously.
- Privacy policies must clearly address the right of consumers to remove or restrict the use of their data. GDPR supports the individual right to his or her own data, and is strongly in favor of the "right-to-be-forgotten" in line with the European Court of Justice's decision in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEDP) and Mario Costela González (Case C-131/12.*
- Requests to acquire, store and use consumers' personal information must be laid out in a concise, transparent and easily accessible way.
- The corporation must clearly explain its reasons for asking for the information, in addition to declaring plainly how long the information will be held and what it will be used for.
- Consent protocols must be reviewed and if necessary, updated at every collection point. This would include:
  - Web landing pages
  - Subscriptions content
  - Event registrations
  - Content download pages
  - Hard copy information forms distributed in person (such as at trade fairs *etc.*)
- Parental permission protocols must also be reviewed and possibly strengthened.
- Common practices like sharing or selling personal data may need to be eliminated.
- Technological measures may need to be implemented, like pseudonymization.
- Companies must implement compliance protocols allowing a customer to be removed, including identifying and erasing personal data. Companies must be able to supply a report of the consumer's personal data on demand, showing removal or revision as requested.
- Corporations should further decide if they will treat EU and non-EU residents differently, or consider all consumers as under GDPR and completely convert their operations.

Get Ready for GDPR Now

American companies that touch the data belonging to EU residents need to ramp up quickly to take measures to adapt to the new world of privacy and data.

As demonstrated by the countdown clock on the GDPR home page, enforcement time will be here shortly. Corporations need to be ready by May 2018, not beginning this process in May.