D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

JANUARY 2012

ADVERTISING, MARKETING & PROMOTIONS

>>ALERT

EUROPEAN COMMISSION PROPOSES COMPREHENSIVE REFORM OF EU DATA PROTECTION RULES

It has been approximately 17 years since the European Commission enacted its Data Privacy Directive governing the processing of personal data of EU residents. Obviously much has changed since that time, including the explosion of access to broadband internet access, smart phones and consumers' online activities and behavior.

With the goal of updating outdated standards, simplifying a complex legal system and providing individuals with more certainty about their personal data, the EU is proposing significant changes to the 1995 data protection rules that, when they become effective, will affect virtually every company doing business in any of the 27 EU Member States – even if a company that processes "personal data" of EU residents is located outside of that geographical area.

The proposed regulation eliminates the differences in the way that Member States have implemented the existing standards by creating a single set of rules governing the use and processing of personal data. The Commission expects that its proposal will be finalized by the European Parliament and EU Member States (meeting in the Council of Ministers) by the end of this year, and that it will take effect two years after that.

KEY TERMS

The proposed regulation contains a number of important definitions. A "data subject" is an identified natural person or a natural person who can be identified, directly or indirectly, by reference to an identification number, location data, or online identifier (including an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. "Personal data" is any information relating to a "data subject," and can include photos and social media postings.

A "controller" is any person or entity that determines the purposes, conditions and means of the processing of personal data. Data is "processed" when "any operation or set of operations" is performed on it, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

THE BOTTOM LINE

Should the European Commission's proposal become law, companies operating in the EU or collecting data from EU residents will need to reassess their privacy practices and in many cases implement new procedures. It remains to be seen in what form these proposals will ultimately be enacted and whether these concepts will migrate to the United States and other jurisdictions.

CONSENT

Under the Commission's proposal, a person's consent to have personal data processed must be specific, informed and explicit and must be reflected either by a statement or by a clear

>> continues on next page

affirmative action that signifies the person's agreement to having his or her personal data processed. This means that an individual's consent to have their personal data processed cannot be implied, whether through behavior or otherwise. A person has the right to withdraw consent at any time.

RIGHT TO BE FORGOTTEN

A unique concept which has garnered much attention leading up to the release of the proposals is the so-called "right to be forgotten," which permits a person to require the erasure of personal data, and to block further dissemination of that data, for a variety of reasons. Among the permitted reasons: that the data is no longer necessary for the purposes for which it was collected; the person withdraws their prior consent; or the person objects to the continued processing of the data. Generally speaking, the erasure must be carried out "without delay."

Moreover, the proposal requires that where a data controller has made the personal data public, it must take "all reasonable steps, including technical measures," to inform third parties that are processing the data that the person requests them to erase any links to, or copy or replication of that personal data.

DATA BREACH NOTIFICATION

While many EU privacy practices differ from those in the United States, in one instance the EU is adopting a United States-created concept – security breach notification. In the event of a security breach leading to the accidental or unauthorized disclosure of, or access to, personal data that is transmitted, stored, or otherwise processed, the appropriate supervisory authority must be notified "without undue delay" and, where feasible, not later than 24 hours after the company becomes aware of the breach. This timing requirement is more stringent than comparable notification requirements in the United States. This notification must describe the nature of the personal data breach, communicate the identity and contact details of the company's data protection officer or other contact point where more information can be obtained, recommend measures to mitigate the possible adverse effects of the breach, describe the consequences of the breach, and describe the measures proposed or taken to address the breach.

In addition, when a personal data breach is "likely to adversely affect the protection of the personal data or privacy of the data subject," the company must communicate the personal data breach to the data subject without undue delay. That communication must describe the nature of the breach, communicate the identity and contact details of the company's data protection officer or other contact point where more information can be obtained, and recommend measures to mitigate the possible adverse effects of the breach.

DATA PORTABILITY

Another unique concept in the proposal is the "data portability" right. According to the Commission's proposal, that means that a person has the right, where personal data is processed by electronic means and in a structured and commonly used format, to obtain a copy of the data. The person also has the right to transmit that data in an electronic format "without hindrance" from the company from which the data is withdrawn. As a result, individuals must have the right and ability to move their data between comparable services, such as different social networking providers. A service provider cannot irrevocably bind the individual's data to their service.

>> continues on next page

PRIVACY BY DESIGN

In another instance of following the trend in the United States, the EU is adopting the "privacy by design" and "privacy by default" principles previously set forth by the FTC in its proposed privacy framework. The concept requires data protection safeguards to be built into products and services from the earliest stage of development, and privacy-friendly default settings will have to be the standard.

Toward that end, the proposal provides that where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf "shall carry out an assessment" of the impact of the envisaged processing operations on the protection of personal data.

ENFORCEMENT

Under the new proposal, there will be only one set of data protection rules and one responsible data protection authority – the national authority of the Member State in which the company has its main establishment. This so-called "one-stop-shop" should be a big benefit to companies struggling to comply with the requirements of multiple regulatory authorities.

PENALTIES

Along with the many new requirements, some significant teeth have been added to the enforcement regime. Under the proposed regulation, the national supervisory authorities may send a warning letter for first offenses. For more serious violations, such as processing sensitive data without an individual's consent or on any other legal grounds, supervisory authorities "shall impose" penalties up to €1 million or up to 2% of a company's global sales. The fines start at €250,000 or up to 0.5% of sales for less serious offenses, such as a company charging a fee for requests from a user for his or her data, and move up to €500,000 or up to 1% for not supplying information to a user or for not having rectified data.

OTHER PROVISIONS

There are numerous other provisions in the proposed regulation, including those relating to the processing of personal data of a child below the age of 13 and the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, among other categories. Companies are required to adopt policies and implement "appropriate measures" to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the regulation. There also are documentation retention requirements, a requirement for organizations of a certain size to appoint a data protection officer (i.e., a Chief Privacy Officer), and specific requirements imposed on data "processors."

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
T: 212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com