Freeborn

Your Future Is Our Purpose

GDPR: A Four-Letter Word?

by Rita W. Garry

A FREEBORN & PETERS LLP CLIENT ALERT

ABOUT THIS CLIENT ALERT:

On May 25, 2018, the General Data Protection Regulation ("GDPR") will take effect in the European Union ("EU). This regulation will apply to all companies, wherever located, that collect, process, or monitor "personal data" of users located within the EU. GDPR requires companies to be responsible for, and be able to demonstrate compliance with the GDPR principles governing personal data processing. Data is a critical element for nearly every business. With GDPR, companies need to assemble business, technology, and legal teams to prepare for this new data management regime.

Enterprises that control or process the personal data of data subjects located in the 28[1] countries of the European Union (or that plan to do so) need to be compliant with the new General Data Protection Regulation (GDPR) by May 25, 2018. The GDPR heralds the most significant reform in personal data protection laws in the EU in over 15 years and will have significant impact on US businesses.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) of 1995. The regulation was adopted on April 27, 2016. It becomes enforceable from May 25, 2018 and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

The GDPR EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom (pending Brexit negotiations)

the EU, thereby aiming to simplify regulatory compliance for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 4% of worldwide turnover.

The main components and questions of GDPR are:

- What is it?
- Scope of regulated "Person Data"
- Does GDPR apply to you?
- Record of processing
- Governance and accountability
- Potential fines and consequences of non-compliance

Unlike the 1995 data protection directive, GDPR is a regulation that will apply directly in all the member states (MS) in the EU in less than a year. Personal data is broadly defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person…" Data subjects cover consumers, end users, customer contacts, patients, employees, contractors, business partner contacts, supplier contacts, and more, based on the territorial scope of DGPR. Thus, the regulation applies regardless of where personal data is controlled or processed (inside or outside of the EU) if the data subject is in the EU and also regardless of whether or not the data subject has entered into a commercial transaction (i.e., make a payment) or whose behavior is simply being monitored where the behavior takes places in the EU[2].

GDPR application is very broad and will apply to US based individuals and companies that are present in the EU and those that, even if not physically present in the EU that (i) control or process personal data; (ii) offer good/services to EU data subjects; and (iii) monitor the behavior of EU data subjects. The GDPR's territorial approach requires enterprises to ask the question of where does the data subject "sit". If they "sit" in the EU and the enterprise does deploy a "geo-blocking" or other forms of restrictions to prevent the collection and/or processing of any personal data of a person located in the EU, then GDPR likely applies to their operations.
Upon a determination of GDPR application, all levels of an organization (operational, technical, executive, and board) must engage in a focused conversation about the nature of its data gathering, data flows and location, data usage, data storage and retention, tracking practices, data accessibility, and overall data management to achieve and demonstrate good governance and accountability to the 'supervisory authority (SA);' meaning an independent public authority established by a MS. These analyses will determine whether the enterprise must designate a representative in one of the MS of the EU and whether it is necessary for the enterprise to designate a Data Protection Officer (DPO).

[2] Profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." Article 3 (4).

GDPR compliance depends, in large measure, on an enterprise's commitment to developing and executing on a "records of processing" program that will pass the scrutiny of auditing SAs. This process will start with data mapping that will best record and visualize the enterprise's data processing activities. With data residing on numerous and multiple devices, in the cloud, on servers in various countries; the first question to building the record must be, "where is our data?" Then, apply the 5-Ws of Who, Where, Why, When, and What to personal data flows. These records should produce a map that identifies the controllers (those that decide the purpose and means of personal data collection), the processors (internal and third parties), a description of the data so collected/processed, the reasons for having the data, the recipients of the data, how data is transferred, the time limits for erasure, and the technical and organizational security measures used in the process.

The record of process is not only important for proving good governance and accountability, but also essential to affecting the data subjects' rights under GDPR without undue delay and in any event within one month of receipt of the request, including:

- Right of Access (Article 15)
- Right of Rectification (Article 16)
- Right to Erasure (right to be forgotten) (Article 17)
- Right to Restriction of Processing (Article 18)
- Right to Confirmation of Rectification and/or Erasure (Article 19)
- Right to Data Portability (Article 20)
- Right to Object (Article 21)
- Right to not be Profiled (Article 22)

As a matter of best practices, the enterprise will develop a "playbook" for each scenario where an EU rightsholder seeks to exercise any of these GDPR rights.

While GDPR is built on the concept of "privacy" and the rights and freedoms of natural persons, it also demands "security" be a central part of compliance. It imposes data breach notification requirements which some experts deem to be the most problematic in terms of compliance. With the proliferation of the types and characteristics of hacking, be it ransomware, phishing, spoofing, or even an innocent loss of data due to offline servers, it is critical to do risk assessments and to develop breach playbooks for each potential type of incident.

Last, but certainly not least, are the fines and other consequences of non-compliance. GDPR uses a two-tiered sanctions regime. Breaches of some provisions by businesses, which law makers have deemed to be most important for data protection, could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater, being levied by data watchdogs. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover, whichever is greater.

Freeborn

Your Future Is Our Purpose

ABOUT THE AUTHOR

Rita W. Garry
Senior Counsel

Chicago Office
(312) 360-6581

rgarry@freeborn.com

Rita serves as Senior Counsel and is a member of the Corporate Practice Group. She specializes in corporate and business enterprise law, including M&A, business sales, joint venture, corporate governance and succession planning, securities, finance, private placements and crowd funding.

GDPR is forcing the conversation among the business, legal, and technology teams within the enterprises within its reach. Compliance will require lengthy and substantive discussions about data mapping from the front to the back-end of its operations from the point of view of the data subjects and the construction of enterprise specific playbooks for all likely scenarios. Please contact your Freeborn & Peters contact to discuss assessing your business' GDPR compliance needs and implementing a privacy and security management program for your business.

ABOUT FREEBORN & PETERS LLP

Freeborn & Peters LLP is a full-service law firm, headquartered in Chicago, with international capabilities and offices in Springfield, Ill.; Richmond, Va.; New York City; and Tampa, Fla. Freeborn is always looking ahead and seeking to find better ways to serve its clients. It takes a proactive approach to ensure its clients are more informed, prepared and able to achieve greater success – not just now, but also in the future. While the firm serves clients across a very broad range of sectors, it has also pioneered an interdisciplinary approach that serves the specific needs of targeted industries.

Freeborn is a firm that genuinely lives up to its core values of integrity, effectiveness, teamwork, caring and commitment, and embodies them through high standards of client service and responsive action. Its lawyers build close and lasting relationships with clients and are driven to help them achieve their legal and business objectives.

For more information visit: **www.freeborn.com.**

CHICAGO
311 South Wacker Drive
Suite 3000
Chicago, IL 60606
(312) 360-6000
(312) 360-6520 fax

NEW YORK
230 Park Avenue
Suite 630
New York, NY 10169
(212) 218-8760
(212) 218-8761 fax

SPRINGFIELD
217 East Monroe Street
Suite 202
Springfield, IL 62701
(217) 535-1060
(217) 535-1069 fax

RICHMOND
411 East Franklin Street
Suite 200
Richmond, VA 23219
(804) 644-1300
(804) 644-1354 fax

TAMPA
1 Tampa City Center
201 North Franklin Street
Suite 2150
Tampa, FL 33602
(813) 488-2920