IndraStra
www.indrastra.com | ISSN 2381-3652

Understanding the DNA of EU's GDPR

indrastra.com/2018/04/Understanding-the-DNA-of-EU-s-GDPR-004-04-2018-0021.html

By IndraStra Global Editorial Team

On May 25, 2018, a new data protection regulation touted as **General Data Protection Regulation (GDPR), Regulation (European Union - EU) 2016/689**, will come into force in the European Union (EU) and its 28 Member States. It will replace the **1995 EU Data Protection Directive 95/46/EC**.

The GDPR will have a significant impact in protecting the data and digital footprint of users of apps and another digital platform. It will provide significant new data privacy protections for individuals residing in EU states.

Although in 1995 the *Data Protection Directive* set an unprecedented foundation for personal data protection, in 2012, the EU proposed a reform of data protection rules because protection has not remained current through the immense technological advances that have taken place since. Furthermore, the nature of the legislation has prevented every EU Member State from implementing uniform standards across the board.

Two main reasons were given by the EU Commission for introducing the reform package for data protection legislation in the Union, namely the differences in the implementation of the existing EU data protection framework in the member states and legal uncertainty

concerning how to deal with the significant risks associated, notably, with online activity.

Data protection is so important to European citizens that the EU requires foreign entities—particularly the United States, where most technology companies are headquartered—to adhere to its stringent requirements. The U.S.-EU Safe Harbor Framework ("*Safe Harbor Framework"* or *"Safe Harbor"*) was created by the U.S. Department of Commerce working with the European Commission (EC) as a means of implementing the *"adequacy"* framework adopted by the European Union's Data Protection Directive. To qualify for membership in the program, an organization could either join a self-regulatory privacy program that already adhered to the requirements, or it could develop its own self-regulatory privacy program in conformance with the framework. The compliance was monitored by adherence to the seven Safe Harbor Privacy Principles, which are: *(1) notice; (2) choice; (3) onward transfer; (4) access; (5) security; (6) data integrity;* and *(7) enforcement.*

But in the case of GDPR, it has retained the core principles of the *Data Protection Directive* but has beefed them up. The core rules may look familiar to experienced privacy practitioners, but this is a trap for the unwary as there are many important new obligations as well as a tougher regime of sanctions for getting this wrong.

Some areas for consideration are:

Accountability (relevant GDPR article, **"Principles relating to the processing of personal data"** – Companies must ensure and adhere to data protection principles and best practices.

Notification (relevant GDPR article, **"Notification of a personal data breach to the supervisory authority"**) – Companies must report data breaches within 72 hours to both the supervisory authority and to those directly affected by the breach. Failure to report properly and fully within 72 hours may result in fines of up to €20 million, or four percent of global annual revenue.

Technology (relevant GDPR article, **"Data protection by design and by default"**) – Companies must establish internal strategies and take the necessary steps to ensure data protection through technology (by design) and as a standard approach (by default)

The text of the new articles in the GDPR grants users, *inter alia*, new rights, and creates the European Data Protection Board.

Article 7 provides conditions for consent;

Article 15 creates a right of access for the data subject;

Article 16 produces a right to rectification;

Article 17 forms the bread and butter of the right to be forgotten and to erasure;

Article 20 informs the right to data portability;

Article 21 discusses the right to object to the processing of one's personal data for direct marketing;

Article 22 explains profiling and the new measures put into effect;

Article 68 sets up the European Data Protection Board; *and*

Article 70 describes the tasks of the newly formed Board

The Existing Confusion

According to the legal experts, the GDPR conflates the two terms under article 17, which is titled *"Right to erasure ('right to be forgotten'),"* there are debates as to whether the right to be forgotten and the right to erasure represent the same idea. According to one legal expert, the right to erasure and the right to be forgotten are interchangeable terms. Another legal expert argues that the two do not represent the same idea, as the right to be forgotten includes data *"that does not breach any norm."* Such a norm could be any general provision of the Directive or Regulation. The right to erasure *"allows data subjects to request the elimination of their personal data when its retention or processing violates the terms of the directive, in particular (but not exclusively) because of being incomplete or inaccurate."* On the other hand, enforcing the right to be forgotten would cause deletion of personal information regardless of whether the information proved harmful or was illegally processed.

The Liability Factor

The GDPR continues the tradition of the supervisory authorities under article 51, but for the first time provides two definitive levels of administrative fines under article 83.96 Now, fines could range from 10,000,000 and two percent of the company's total annual turnover, or anywhere from 20,000,000 to four percent of the company's annual turnover, whichever is higher in either case. To put these numbers into perspective, consider Google's revenue, which was $74.5 billion in 2015. A range from two percent of its turnover to four percent would be from $1.49 billion (1.43 billion) to $2.98 billion (2.85 billion). Money talks: the new enforcement mechanism certainly discourages indifference and encourages compliance.

To avoid GDPR liability, organizations should, among other things, establish and implement policies and procedures regarding their protection and handling of the data of individuals that they control/obtain, conduct staff training, hire DPOs, and establish breach response protocols. These measures can help identify, prevent, and reduce regulatory and/or legal liability. Companies should review all contracts with business partners to ensure compliance with the GDPR and review insurance policies to make sure that GDPR-related coverage is in place. In addition, organizations should keep records of GDPR

organizational and technical measures that have been implemented. This will be useful in the event of an audit by a supervisory authority.