Published on *The National Law Review* https://natlawreview.com

What is GDPR and Why You Should Care

Article By:

Gene Markin

The European Union (EU) has long recognized the importance of privacy as a human right. In 1980, the Organization for Economic Cooperation and Development (OECD) issued the "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data," which laid out seven principles governing the OECD's recommendations for protection of private personal data. These principles were then incorporated into the EU's Data Protection Directive, which regulated the processing of personal data and was officially adopted in 1995. The principles included:

- *Notice*: data subjects should be given notice when their data is being collected;
- *Purpose*: data should only be used for the purpose stated and not for any other unstated purposes;
- *Consent*: data should not be disclosed without the data subject's consent;
- *Security*: collected data should be kept secure from any potential abuses;
- *Disclosure*: data subjects should be informed as to who is collecting their data;
- *Access*: data subjects should be allowed to access their data and make corrections to any inaccurate data; and,
- *Accountability*: data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

In 2012, the European Commission (EC) announced their plans to unify data protection law with goals which included: the harmonization of 27 national data protection regulations into one unified regulation; the improvement of corporate data transfer rules outside the EU; and the improvement of user control over personal identifying data. This proposed legislation was the General Data Protection Regulation 2016/679 (the "GDPR"), which was adopted by the EU in April of 2016, with a set implementation date for the end of May 2018.

This new update superseded the existing language in the Data Protection Directive, and added

requirements and provisions to the processing of “data subjects” and their personally identifiable information. One of the largest changes was the new directive that the legislation would “apply for all non-EU companies without any establishment in the EU, provided that the processing of data is directed at EU residents.”

This meant that GDPR applies to all companies or organizations inside the European Union as well as those outside of the EU that collect, store, process, or use EU residents’ data. Thus, any U.S. based business that interacts with EU residents is affected by this legislation. Specifically, any and all companies that have clients (or believe they may have clients) with EU residents are subject to the GDPR. Any business that does not comply with GDPR regulations could find themselves hit with a fine of up to 4% of their global annual revenue. In order for any U.S. company to comply, they must have policies in place that comply with GDPR’s policies, including:

- Allowing customers to see and delete the data that concerns them;
- Providing notice of data breaches within 72 hours;
- Making data policies transparent to an average person (*e*., not hiding privacy information in an overcomplicated manner that a layperson could not understand);
- Hiring a Chief Data Officer if necessary for their business and data constraints; and,
- Following the original seven principles of the Data Protection Directive.

Additionally, and most significantly, each person must provide explicit “opt-in” consent in order for a business to process and obtain that person’s personal data and be allowed to revoke this permission at any time. Furthermore, any processor of personal data *must* disclose any data collection, the purpose for the data processing, how long the data is being retained, and whether or not it is being shared with any third-party organizations outside of the EU.

Not surprisingly, an Austrian privacy attorney has filed multibillion-euro seeking complaints against several global platforms, including Google, Instagram, Facebook, and WhatsApp, only days after the General Data Protection Regulation (GDPR) went into effect on May 25. These suits will be some of the first cases to test the reach of the new regulation and accuse the companies of seeking “forced consent” in their terms of service and seek the maximum penalties against Google in French courts, Instagram in Belgium, WhatsApp in Germany, and Facebook in Austria, for a total of 7.5 billion euros.

The complaints allege that these platforms pressured users to comply by “bombarding” them with pop-up windows online or in applications, and often threatened that the service could not be accessed without consent.

Many more suits are anticipated now that the GDPR is in full effect.

National Law Review, Volume VIII, Number 240