The Top 10 Things to Know About GDPR

By Steven J. O'Neill, Esq.

DAYMARK
Navigate information technology

10. What is GDPR?

GDPR (European Union General Data Protection Regulation) is a comprehensive new law protecting the data privacy of EU citizens. Enforcement begins on May 25, 2018. It consists of 99 articles and will have sweeping impact on U.S. enterprises. It requires that all personal data be handled according to the GDPR Data Protection Principles. These includes the famous right to be forgotten, as well as transparency, data portability, and information security.

9. Who does GDPR protect?

The GDPR protects "personal data" of EU citizens. So, if you are only doing business outside the European Union then you don't have to consider it at all, right? Think again. What about any business with a website? What about an app or game?

The upshot of a new privacy and data security regulation of this scope and breadth is that non-EU companies must either comply or forego the market. Outside of the EU, this regulation will impact call centers, sales management, advertising and promotion campaigns, marketing and customer relationship management, data processing including cloud computing, SaaS, IaaS, R&D, information security management, and information governance (IG).

8. What data does GDPR protect?

The GDPR defines personal data as "any information relating to a data subject." (Article 4(1)). A data subject is not only a person who is actually identified by the data but is also a person who is *identifiable.*

A person is identifiable if he or she "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, economic, cultural or social identity" of that person. (Article 4(1)).

Personal Data is broadly protected including details about a person's family, lifestyle, medical condition, genetics, education, training, employment, finances, contracts, IP addresses, cookie identifiers, RFID tags, website use, search history, and any other data that would be commonly understood as being personal.

Without special protections, GDPR prohibits the processing of personal data that reveals: race, ethnicity, politics, religion, philosophy, trade union membership, genetic data, biometric ID data, health data, sex life, and sexual orientation. Processing of this data is governed by strict limiting provisions in Article 9(2).

7. When does Personal Data require protection?

According to a Working Group (W29) analyzing the impact of the GDPR, personal data that must be protected must implicate at least one of three elements:

- **Content:** Information that is about a particular person regardless of the purpose of the data or the potential impact of the data on that person is covered.
- **Purpose:** When data is or can be used in a way that can impact or influence the behavior of an individual, it is covered.
- **Result:** When the use of data is likely to have an impact on a person's rights and interests. For example, a gig-economy phone app tracks a person's location ostensibly to provide better service and allow the app's developers to improve the software. The app hypothetically contains evidence of: speeding, visiting marijuana dispensaries, and engaging in political demonstrations, perhaps resulting in termination of employment. Under the result element, it is covered.

6. Data Controllers vs. Processors

Under the GDPR, controllers of data have more obligations than processors of data. However, processing of data is very broadly defined as carrying out any operation or set of operations on the data, including:

Collection	Recording	Organization
Structuring	Storage	Adaptation or Alteration
Retrieval	Consultation	Use
Restriction (marking as subset)	Erasure	Destruction
Disclosure by transmission	Dissemination	Alignment or combination

Obviously, almost any conceivable processing or storage of data is covered. Controllers have the auditable obligation to ensure that all their processors and sub-processors follow the GDPR Principles.

5. What are the GDPR Data Protection Principles?

Both data controllers and data processors must comply with the GDPR Article 5 principles when processing personal data. Article 5 includes the following data protection principles:

- **Lawfulness, fairness and transparency**. (Article 5(1)(a)). Transparency reflects the notion that EU citizens have rights to knowledge of their personal data and a meaningful understanding of its impact upon them. The requirements for lawful processing are in Article 6.
- **Purpose limitation**. (Article 5(1)(b)). Personal data can be collected for specified, explicit, and legitimate purposes only. It cannot be processed in any way that is inconsistent with those purposes or enlarges those purposes. Think about the EU equivalent of Cambridge Analytica's harvesting of Facebook user data or just banner website ads.
- **Data minimization**. (Article 5(1)(c)). Similar in concept to Massachusetts' and other jurisdictions' mandate that the amount of data collected be kept to a necessary minimum, the GDPR requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. It is not appropriate for data controllers to collect information just in case a future need might arise. (Think server logs.)
- **Accuracy**. (Article 5(1)(d). Not only must personal data which is collected and processed be accurate but it must be kept up to date. If inaccurate for its purposes, it must be rectified or erased without delay.
- **Storage limitation**. (Article 5(1)(e)). Personal data must not be kept in a form in which data subjects can be identified from the data for longer than is necessary to accomplish the purpose. Longer periods are allowed for archiving purposes in the public interest or for purposes of scientific, historical or statistical research. These longer-term purposes are subject to data security safeguards.
- **Integrity and confidentiality**. (Article 5(1)(f)). Technical and organizational security safeguards are required to ensure protection against unauthorized/unlawful processing and against accidental loss, destruction, and damage.
- **Accountability**. (Article 5(2)) The data controller is responsible for and must document compliance with the data protection principles. This principle is critical because it requires data controllers to enforce and audit the effective application of the other principles with all data processors. Non-EU companies must analyze whether they "touch" a sufficient quantity of EU personal data records such that the GDPR is triggered. This could occur in a wide variety of examples such as payroll service, call center, medical records service, server hosting company, or app developer.

4. What is Lawful Processing?

A data controller must be able to justify that the processing of personal data is lawful. Article 6 sets up a regime of legal grounds focused on the basic concept of freely given, informed, opt-in consent. The consent must be for specific purposes, necessary for the contract with the data subject. Article 4(11) defines consent as a "freely given, specific, informed and unambiguous" indication of the data subject's wishes by a statement or by a clear affirmative action. A statement can be in writing, by electronic means, or oral. Examples of affirmative action include: checking a website dialog box; choosing settings for an online service; and any other clear affirmative act of acceptance. (Recital 32, GDPR).

Unlike many current opt-out practices, under the GDPR consent is not implied by silence, pre-selected dialog boxes or the burying of the consent inside the legalese of a Terms of Service statement. Also unlike current practices, the GDPR requires that data subjects have the right to withdraw consent at any time – consent must be as easy to withdraw as to give.

3. What are data subjects' rights?

The GDPR gives data subjects the right to obtain from a data controller access to his or her personal data. Also, the data controller must disclose:

- The specific purposes of the processing of the data
- The categories of personal data involved
- The recipients or type of recipient of the personal data, especially recipients in third countries or international organizations
- Period of anticipated storage of data
- A statement of the right to request correction of, restriction on the processing of, or the erasure of the data – this is the "right to be forgotten" in Article 17
- The statement of the right to file complaints about the processing with the appropriate authorities
- Source information on the personal data that was not collected from the data subject
- Information about automated decision making, including profiling, together with meaningful information about the logic involved and the possible consequences to the data subject of such profiling
- If the data controller or processor transfers personal data to a third country or international organization, they must inform the person of the safeguards put in place – this impacts the right to data portability in Article 20
- The controller must provide a copy of the personal data undergoing processing free of charge – generally in format that is readable without specialized software tools

Breach Notification. Another key provision of the GDPR is a mandate that information breaches be reported within 72 hours. This is a major change in the way security breaches have been handled. It may be wise to pre-coordinate with law enforcement authorities in order to avoid delays over communications and jurisdictional issues. Data breach "fire drills" are advised.

2. What are some other obligations of controllers and processors?

Unlike the prior European Data Protection Directive, the GDPR places significant new burdens on the data processor, as well as requiring effective audit trails by the controller to promote the key principle of accountability.

The controller must have legally binding contracts with data processors imposing the following obligations:

- Limit processing only to the documented instructions
- Because of concern with third country and international organization transfer, the instructions should clearly define any authorized cloud computing use
- Comply with information security obligations imposed on controller in Article 32 of the GDPR

- Require that all data processor staff with access to the personal data have a written confidentiality agreement or statutory obligation
- Not to assign or subcontract to another sub-processer without the prior written consent of the controller
- Assist the controller in carrying out its obligations to the data subjects such as access and the right to be forgotten
- Assist the controller with its data security obligations in Articles 32 and 36 of the GDPR

Significant numbers of processors based in the U.S. who handle the personal data of EU citizens have been impacted by this contractual flow-down provision.

1. What are the penalties?

The law has teeth. It authorizes administrative fines on controllers and processers (Article 83) reaching up to 20 million Euros (roughly $24M) or 4% of annual revenue (whichever is higher). It also authorizes a private right of action, which will be fleshed out on a country by country basis as time passes.

About the Author:

Steven J. O'Neill is an experienced litigator with extensive knowledge of computer data systems architecture, electronic records issues and e discovery law. He has presented numerous seminars on these topics throughout the U.S. His practice areas include business law, litigation and technology law focusing on e discovery, Information Governance, Privacy, and Information Security Compliance. He is admitted to practice in state and federal court in MA and CT and available to serve clients nationally. For more information, visit www.attorneyoneill.com.