

The Meaning and Impact of the General Data Protection Regulation: Executive FAQ

By: Tim Walters, Ph.D.

The GDPR Requires Significant Changes for Firms Worldwide

The European Union's General Data Protection Regulation (GDPR) will substantially impact any company that (a) sells to EU residents, or (b) "monitors" the behavior of EU residents. Compliance will require significant changes in how companies collect, store, process, share, and transfer personal data. Failure to comply carries very high fines, as well as the possibility of consumer class-action lawsuits and the threat of imprisonment for responsible executives.


Firms must be fully prepared when the law goes into effect on May 25, 2018; the "grace period" is now. An adequate response requires C-level (and even board-level) attention and involvement immediately.

The Essentials of GDPR Compliance in Six Questions and Answers

Here are the top six things executives need to know about the GDPR in order to get started with a compliance strategy and program.

1. Does my company have to comply with the GDPR?

Make no mistake: The GDPR is *not* restricted to European companies, nor to global firms with a European presence. The regulation does not aim to control activity within a specific geography. Rather, it is intended to protect the privacy and personal data rights of EU residents.¹ Thus, the law applies to any company that collects and/or uses any such personal data, regardless of the company's size, location, or legal residence.



Specifically, the GDPR names two broad activities that, if engaged in by any non-EU firm, will trigger the application of the GDPR and compel compliance:

- **Collecting and using personal data when offering goods and services.** Any company that offers goods or services to any EU resident (“irrespective of whether a payment . . . is required”) must comply with the regulation.²
- **Collecting and using personal data when monitoring behavior.** Even in the absence of a commercial offer, the regulation controls the activities of any firm that “monitors” the behavior of EU residents. This is a very far-reaching provision that potentially applies to any company with a website that tracks visitors’ behavior and actions for the purpose of mundane web analytics – if that site is accessible to EU residents and in any way collects personal data.³

It is important to note that the GDPR applies equally to what it calls data controllers and data processors. Data controllers request and collect personal data and determine how it will be used. Data processors “process personal data on behalf of the controller.”⁴ This means, for example, that a cloud service provider that stores, analyzes, transfers, or conducts virtually any operation on personal data on behalf of a client (the data controller) is required to comply with the GDPR.⁵

2. What counts as personal data?

The GDPR replaces an EU directive issued in 1995, before the commercial web and the digital era. One of its primary aims, therefore, is to catch up with and regulate the digitization of personal information. Thus, the GDPR specifically designates “online identifiers” such as IP addresses, browser cookies, and radio frequency ID tags as personal data. There is also a category of “sensitive data” that requires especially careful handling, including information about “racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation.”⁶

However, the GDPR does not include an exhaustive list of what does or does not qualify as personal data. Rather, the regulation defines personal data as “any information relating to an identified or identifiable natural person.”⁷ This broad and flexible definition will prevent firms from inventing and using new types of identifiers, such as “device fingerprinting,” that are not specifically named in the regulation.⁸

Make no mistake: The GDPR does not apply only to EU firms or multinationals with a European presence.

3. What are the consequences of non-compliance?

The GDPR authorizes data protection authorities to impose fines that are “effective” and “dissuasive.” That is, the fines are meant to be painful, in order to discourage repeat offenses. At the highest level, authorities may fine companies 20 million euros or 4% of their *global* turnover, whichever is greater. (By way of illustration, 4% of Google’s 2015 global turnover is about \$3 billion.) Fines may be levied for each violation; presumably repeat offenders will receive higher and more “dissuasive” fines.

In addition, citizens may file complaints or initiate lawsuits, either individually or in class actions. Numerous privacy advocacy groups have already announced plans to closely monitor the data practices of businesses as soon as the regulation becomes enforceable. Given the stakes involved, it is likely that firms will also monitor each other’s behavior as a form of competitive intelligence.

The regulation directs authorities to take numerous factors into account when deciding whether to impose a fine and, if so, how large it should be. Among these are evidence of a firm’s good-faith attempts to properly govern data collection and usage, such as conducting data audits, reviewing processes for handling personal data, and carrying out privacy “impact assessments” prior to data processing. This means that the attitude of “we’ll cross that bridge when we get to it” could result in very high bridge tolls. The GDPR demands C-level and potentially board-level attention *today* in order to ensure compliance in 2018.

The fine for non-compliance with the GDPR can reach €20 million or 4% of the firm’s global turnover, whichever is greater.

4. What are the major provisions of the GDPR?


The GDPR will require firms to adopt fundamentally new processes and strategies in any area that touches upon personal data. It contains substantially new or expanded requirements and restrictions on the collection, use, storage, sharing, transfer, and ultimate destruction of data. The key provisions are too numerous and extensive to summarize here. There are two areas that firms may find most shocking and disruptive:

■ Data minimization and data protection

by design: Data is, famously, “the new oil.”

Marketing and customer experience practices as they have evolved over the last ten years – especially under the banner of big data – have pursued a policy of “data maximization.” That is, the advised approach is to get as much data as you can – directly from consumers, through behavioral monitoring, from internal systems, from third parties, etc. – then treat it as a corporate asset and extract as much value out of it as possible. This could include reusing it for various purposes or even selling it to another party.

In direct contrast, the GDPR requires that firms adhere to a principle of “privacy by design and default.” This means that, instead of data maximization, firms must pursue a policy of *data minimization*. Specifically, a firm must be able to demonstrate – upon request, or in some cases in advance – that it has designed a data processing system that uses the *smallest*



possible amount of personal data for the *shortest* possible period of time and deletes the data as *quickly* as possible after the processing (for that *specific* purpose) is completed.

In short, data protection by design requires every affected firm to review and potentially to redesign every single business process that uses personal data.

- **Data portability and “the right to be forgotten.”** The GDPR stipulates that any individual (a “data subject”) can at any time ask a company or organization for a *complete report* of all personal data it holds about that individual. The subject can request a copy of that data, which must be provided in a reasonable time and in a “commonly used and machine-readable format.” Individuals can at any time direct the company to delete or destroy all of their data. (This is the so-called Right to Erasure or Right to Be Forgotten.)

Finally, an individual can demand that a company send all of the relevant personal data they hold to another data controller. That means that if I have purchased personal insurance from, say, AXA, I can have them pack up everything they know about me and my insured property and send it to a competitor such as Prudential.

The provisions for data portability will do for personal data what mobile number portability did to network operators. It opens up an entire new vector for competition and competitive advantage or disadvantage. Innovative companies will find ways to induce consumers to switch not only their businesses but also their potentially rich data profile – and thus weaken the previous provider as well.

5. What part of the organization should take charge of compliance?

Unsurprisingly, most firms assign compliance professionals to lead the initial investigation of the GDPR.

However, it is crucial to realize that the GDPR requires, and expects, a systematic, coordinated response across numerous business units and skill sets. For example, a new marketing campaign involving personal data will require, at minimum, the attention of marketing (to design the campaign), IT (to create and validate the data processes), legal (to draw up and approve the consent requests), HR (to ensure appropriate training), a designated data protection officer (for oversight and governance), and top executives or the board of directors (who must determine the balance between the risks and benefits of using various types of personal data).

The requirement for “data minimization” will require every affected firm to review and potentially redesign every business process that uses personal data.



In short, the GDPR is not a problem for legal, it's not a problem for IT, it's not a problem for security and risk, it's not a problem for marketing, and it's not a problem for the board of directors. It's a problem for *all of them*, and it requires a systematic, strategic response.

6. What should we do to get ready for the GDPR?

Firms need to get a very clear view of what personal data they currently collect and store. A thorough audit should aim to create a complete inventory of personal data including backups, copies, and data that has been shared with partners or others. (Given the complex organization structures, uncoordinated customer engagement efforts, and opaque technical infrastructures in many organizations, this step alone could take months.)

The related and more important step is to understand how data is used in existing business processes. In the current business model, how is personal data monetized or otherwise exploited for business value? How does this current state compare to what is allowed under the GDPR? Where are the deltas greatest, and which should be

addressed first in order to minimize the extent and the duration of the impact?

But before taking either of these vital steps, it's necessary to understand the GDPR itself. Priority must go to a *knowledge audit*. What roles and individuals will be impacted by the GDPR? What is their current knowledge, and how much do they need to know? For example, marketers, product managers, sales staff, HR professionals, and senior executives (among many others) all need to be aware of the GDPR, but the breadth and depth of the required knowledge varies considerably. Thus, the first step in preparing for timely compliance with the regulation is to map out and launch an educational campaign tailored for needs of specific groups in the organization.

The GDPR is a problem not just for legal, or IT, or marketing, or the board of directors. It's a problem for all of them, and it requires a systematic, strategic response.

Endnotes

- 1 The EU Charter of Fundamental Rights grants every EU resident the right to “respect for private life and the right to the protection of personal data.” The EU parliament aims to ensure these rights with the GDPR.
- 2 The final text of the GDPR is available in English and 23 other languages at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT. Regarding the territorial scope of the regulation, Article 3 states (emphasis added): “This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.”
- 3 Recital 24 states: “In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.”
- 4 See the definitions of controller and processor in Article 4.
- 5 Processing is defined in Article 4 as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[.]”
- 6 See for example Recital 75.
- 7 See the definition of personal data in Article 4.
- 8 Device fingerprinting designates a variety of methods for detecting the unique characteristics, settings, and functionality of a device for the purpose of identifying it and tracking it across the web. See for example <http://motherboard.vice.com/blog/device-fingerprinting-can-track-you-without-cookies-your-knowledge-or-consent>.

About Digital Clarity Group



Digital Clarity Group is a research-based advisory firm focused on the content, technologies, and practices that drive world-class customer experience. Global organizations depend on our insight, reports, and consulting services to help them turn digital disruption into digital advantage. As analysts, we cover the customer experience management (CEM) footprint – those organizational capabilities and competencies that impact the experience delivered to customers and prospects. In our view, the CEM footprint overlays content management, marketing automation, e-commerce, social media management, collaboration, customer relationship management, localization, and search. As consultants, we believe that education and advice leading to successful CEM is only possible by actively engaging with all participants in the CEM solutions ecosystem. In keeping with this philosophy, we work with enterprise adopters of CEM solutions, technology vendors that develop and market CEM systems and tools, and service providers who implement solutions, including systems integrators and digital agencies.

Contact Us

Email:

info@digitalclaritygroup.com

Twitter: [@just_clarity](https://twitter.com/just_clarity)

www.digitalclaritygroup.com