Regulatory Transparency Project

Unlocking Innovation & Opportunity

The GDPR and the Consequences of Big Regulation

Cyber & Privacy

Matthew R. A. Heiman (Chair)

The views expressed are those of the author in his personal capacity and not in his official/professional capacities.

To cite this paper: Matthew R. A. Heiman, "The GDPR and the Consequences of Big Regulation", released by the Regulatory Transparency Project of the Federalist Society, July 5, 2018 (https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-GDPR.pdf).

5 July 2018

Table of Contents

I. Introduction

If you have received a flurry of e-mails from vendors and websites asking you to review and accept new data privacy terms and conditions, it's not a coincidence. The European Union's General Data Privacy Regulation (GDPR) went live on 25 May 2018. Passed in 2016 by the European Parliament, the GDPR replaces the Data Protection Directive of 1995. It applies to all EU member countries, but as explained below, it has global reach. The primary purpose of the law is to give individuals greater control over their information by mandating companies and organizations handle that information with greater care. As with most regulation, the stated intention of greater protection and transparency in managing data sounds good, but the costs and consequences are not often discussed by privacy advocates and data protection authorities in the EU.

II. What's New?

The GDPR, made up of 99 articles and 173 preliminary comments, or recitals, contains a number of new provisions that businesses will have to carefully consider to avoid the risk of non-compliance.

From an American perspective, one of the GDPR's most noteworthy aspects is its **extraterritorial reach**. Anyone collecting and processing personal data (name, address, e-mail address, credit card information, etc.) about someone physically located in the EU is subject to GDPR requirements. If a retailer has website with the capacity to accept orders from within the EU, it is likely collecting personal data about its customers, and it is subject to the GDPR.

Obtaining **consent to use personal data** has become much stricter. Consent must be freely given, and it must be unambiguous and specific. The language requesting consent to use personal data must be clear and easy to understand. In addition, it must be as easy to withdraw consent as it is to give it.

An individual has the **right to demand a data inventory**. Companies must be prepared to provide this access to collected personal data in an electronic format as well as confirm whether the individual's personal data is being processed, where it is processed, and the purpose of its use. Sometimes referred to as **data portability**, companies must honor these data requests free of charge and also be willing to transfer the data elsewhere with no cost to the individual.

Under the GDPR, **notification of data breaches to the data protection authorities must happen within seventy-two hours** of discovering the breach. Notification to individuals must occur if there is likely to be a "high risk" to their rights and freedoms. A company must use as many forms of communication as is necessary to deliver the notice timely — telephone, e-mail, and public announcements.

Individuals have the **right to be forgotten**. This means that a company is obligated to delete all personal data when asked to do so by the individual. The company must also take reasonable steps to notify any third parties that the individual has made this request. All requests to be forgotten must be responded to within one month.

The GDPR requires that companies practice **privacy by design**. This means that companies must process only the data that is absolutely necessary to complete the business task. Companies must limit their employees' access to personal data that is necessary to complete the business task. In addition, companies must maintain documentation of their privacy by design practices and conduct a data protection impact assessment for more risky processing.

While the exact size and details are not clear, **large companies** wishing to comply with the GDPR must maintain comprehensive records related to collection, processing, and storage of personal data, and they **must designate a Data Protection Officer** (DPO). The DPO must have sufficient expertise on the subject of data privacy and report to senior management of the company.

Failure to comply with the GDPR in the areas of international data transfers, failure to obtain appropriate consent, and failure to implement privacy by design may result in **significant fines** — up to 4% of annual global revenue or €20 million, whichever is greater. Fines of 2% of annual global revenue or up to €10 million may be imposed on companies that do not have appropriate documentation or fail to notify data protection authorities and individuals of a data breach.

III. What's the Problem?

Proponents of the GDPR argue that individuals now have a greater ability to control their data, and companies that misuse and abuse their access to personal data are at greater enforcement risk. They also argue that the GDPR's extraterritorial reach is raising the data privacy bar for individuals not located in the EU because companies are adopting a single standard for management of data that matches GDPR requirements. While some of this may be true, the GDPR boosters have ignored a number of negative consequences that result from the GDPR.

First, fundamental GDPR terms are vague, such as "collect" and "store." In other instances, fundamental terms are incredibly expansive. "Personal data" is defined as "any information relating to an individual, whether it relates to his or her private, professional or public life." As other observers have noted, the desire to implement the GDPR quickly trumped ironing out some of these key details. Eduardo Ustaran of Hogan Lovells law was quoted in *The Economist* magazine as saying that the law is four to five times more complicated than the existing law, and "[w]e'll probably spend the next 20 years figuring out what it means to be compliant." This is exactly the opposite of what well-drafted and precise laws should look like. While all legal text is subject to interpretation and judicial challenge, a dramatic data privacy regulation that lacks clarity around "collect," "store," and "personal data" has missed the mark, especially when this lack of clarity is coupled with a significant increase in the penalty regime.

Second, like many regulations, the GDPR's complexity and burdens will be most easily borne by the largest actors in the marketplace such as Google, Facebook, and Amazon. These organizations have the resources, the lawyers, and the compliance experts necessary to ensure compliance. Smaller organizations will struggle to meet the GDPR's requirements. A recent survey showed that a company will spend $1 million to acquire the technology necessary to comply. This is peanuts for a large organization, but it is a huge burden for small companies doing business in the EU. For those

that can't afford compliance, they will have to accept the risk of being caught or choose not to serve those in the EU. While large actors can deal with GDPR, and it is billed as a consumer-friendly regulation, it is interesting to note that government organizations, which are responsible for some of the largest data privacy breaches, are not subject to its strictures.

Third, the GDPR threatens the current internet business model, and whether a company is big or small, the costs for this new regime will be passed on to consumers in the form of higher costs and diminished services. Over the past fifteen years, the internet business model has been premised on the exchange of free or heavily subsidized services (e.g. Facebook, LinkedIn, Google, news outlets) in exchange for the use of personal data that allows for targeted advertising. The GDPR has made it much more difficult for companies to continue making this trade with their users. Services like Amazon suggesting products, Netflix suggesting movies, and advertising that is relevant to your life may go the way of the dodo. This may be a good trade for some, but most consumers have been happy to give up a certain amount of privacy in exchange for free apps, free email and messaging services, and free personal and professional networking tools.

Fourth, not only does the GDPR threaten the existing internet business model, but it also poses risks to critical emerging technologies such as blockchain and big data/artificial intelligence (AI). That's because GDPR focuses on collection and storage of data, though those terms are not clearly defined, rather than how the data is used. Blockchain requires that data in the chain remain there permanently. But, under the GDPR, an individual has the right to be forgotten — the right to demand that their data be deleted. Blockchain's distributed ledger architecture also means there is no central DPO overseeing the processing of all of the disparate pieces of data. GDPR also requires deletion of personal data as soon as possible. Again, blockchain does not allow for deletion of such data. This doesn't mean blockchain is dead, but it circumscribes its use, and data will have to be anonymized. This will increase the cost of a technology that offers far greater data protection than all the DPOs in Europe.

Similarly, the use of large swaths of data for AI and big data exercises will become more difficult. As suggested by the term big data, big data requires large amounts of data to develop trending analyses and predictive analytics — elements of AI. To remain compliant with GDPR, companies seeking to work with individual data that forms larger data pools will have to constantly go back to individuals asking for permission to use their data for each new variation. This will create burdensome costs for the company, annoyance to the individual/consumer, and possible collapse of the effort. The answer may be to develop these technologies outside the EU.

Fifth, the GDPR's negative consequences on future technological growth and innovation, particularly within the EU, are in addition to the challenges created for information sharing occurring today. For example, the WHOIS database, which is a publicly available registry of website ownership, is a critical tool for law enforcement investigations and consumer protection. But now, it is unclear whether the registrars of this information may provide publicly website ownership details without first obtaining permission from those owners. Cybercriminals are unlikely to grant such a request. While foreseeable since 2016 and potentially salvaged in part by a "temporary specification,"

this development frustrates the utility of the database, and it is one of many aspects of critical information sharing that happens within the private sector and between the private sector and governments that are now thrown into question because the GDPR provides insufficient guidance.

Finally, some have not unreasonably suggested that GDPR is less about upholding cherished European ideals of privacy than it is a protectionist economic tool. Europe is clearly unhappy with the dominance of U.S. technology firms, which are now being joined by Chinese companies in the war for technological supremacy. U.S. firms have been subject to consumer protection, antitrust, and tax investigations by EU authorities. Proposals have been floated within the EU to tax online transactions. The GDPR will be a boon to European cloud service providers, as movement of EU-user data outside of the EU has become riskier as a result of GDPR. While time will tell whether Europe wields the GDPR cudgel to go after American technology firms, American economic actors should have their eyes wide open.

IV. What's Next?

The GDPR will not go away anytime soon. The best-case scenario is that the EU will use its regulatory mechanism to punish only the most egregious misuses of personal data, its regulators will quickly issue further guidance documents that clarify the lack of detail around fundamental terms in the law, and companies are given credit, particularly based on their size and scope of operations, for good faith efforts to comply.

In the meantime, we should expect the following: the regulatory uncertainty will stifle commercial investment while increasing legal and compliance costs; these costs will be passed to consumers and services will diminish; tech and data entrepreneurs will continue developing and innovating, likely somewhere other than the EU; and individuals should look forward to a steady stream of emails with new and sometimes improved data privacy terms. Big regulation has consequences.