Insight

Explaining the EU's General Data Protection Regulation

WILL RINEHART, ALLISON EDWARDS | MAY 22, 2018

Executive Summary

The European Union's General Data Protection Regulation (GDPR) is set to take effect on May 25th. This new set of privacy regulations is expansive in scope yet simultaneously vague in how it might be implemented. On the whole, it will hurt the dynamism and economic health of the Internet. Because of the fundamentally international scope of the Internet, this regulation is sure to impact companies and consumers across the world, including in the United States.

The GDPR is a wide-ranging regulatory document that includes a variety of obligations and rules:

- Data collection and use must be minimized by any means necessary, which is likely to limit secondary uses and stifle start-ups;
- Users must affirmatively consent to all data processing, a costly requirement that doesn't give consumers any more options;
- Consumers have the right to export their data, a feature already present on the biggest social media platforms;
- Consumers can force search engines to delist certain information under the right to be forgotten, which has many journalists and good government organizations enraged; and
- If companies violate any of the provisions, the fines are exceptionally onerous.

The biggest companies are spending an estimated $7.8 billion to come into compliance with the new European regulation. Some have suggested that Congress should import this legislation wholesale. Adopting this legislation would negatively impact the dynamic market without giving consumers any added protection.

What is the GDPR? Why does it exist?

The General Data Protection Regulation (GDPR) is a set of regulations for the whole of the European Union (EU)that define the data protection rights of individuals and that place consequent obligations on organizations. Formally adopted on April 16, 2016, organizations had two years to comport with the law. So, on May 25th, 2018, the GDPR will become officially enforceable.

The GDPR springs ultimately from the Charter of Fundamental Rights of the European Union. The opening pages of the regulation explain its purpose: "The protection of natural persons in relation to the processing of personal data is a fundamental right." The development of the digital economy and the proliferation of data in the past twenty years caused the EU to establish a new set of laws governing privacy and data.

In contrast to this rights-based approach, the U.S. regime broadly focuses on privacy harm. The resulting legal framework has come to be called the sectoral approach. Under this approach, data is regulated based on the

category into which it falls. Health information is regulated under Health Insurance Portability and Accountability Act of 1996 (HIPAA), financial data is governed under Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), child's privacy is regulated under the Children's Online Privacy Protection Act (COPPA), while marketing can be regulated under the Telephone Consumer Protection Act (TCPA) or the CAN-SPAM Act. While some have chided the United States for not having comprehensive privacy protections, *ex post* regulation by the FTC and the efforts of privacy advocates, professionals, and market forces create a more ambiguous legal environment. Legal scholars Kenneth Bamberger and Deirdre Mulligan call it productive ambiguity. Under this harm-based system, because companies know they have to protect consumers and will face punitive actions if they don't, firms implement substantive protections on their own.

The GDPR replaces the 1995 Data Protection Directive (Directive 95/46/EC). This older directive is one of the two kinds of legislation in the EU, the other being a regulation. A directive is a legislative act that sets out goals that all EU countries must achieve, but the individuals countries have to implement the directive via a national legislative act, which gives them some flexibility. For the 1995 privacy directive, Data Protection Authorities (DPAs) were created in each member state to serve as the local regulatory body. Regulations, on the other hand, apply to the whole of the EU directly. Thus, the GDPR is a binding legislative act that is applied to all countries, so everyone must comply.

The Basics of the GDPR

The GDPR defines and then regulates various kinds of data processing actions as well as actors, so companies can be liable for a range of legal obligations.

Personal data is an especially broad term that includes "any information relating to an identified or identifiable natural person ('data subject')…such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Data processing is similarly defined in an expansive manner to incorporate "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." A data controller is the individual or legal entity that "determines the purposes and means of the processing of personal data." A data processor is the natural or legal person who processes personal data on behalf of the controller. Controllers decide how and why the personal data is going to be processed, and processors process the data on behalf of the controller. In reality, most companies would be considered both a controller and a processor.

From these definitions, the GDPR sets up a number of obligations and rules, which are briefly detailed below.

Data Collection and Use Must be Minimized

Personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." In practice, this means that data processing has to be minimized. Companies will need to be able to prove that the data that is being held is useful to the consumer; otherwise, they are required to delete that information. While it may sound easy, in practice companies have built their data pipelines around the goal of collecting and then mining. As one commenter noted, "Now

companies will need to reverse engineer existing data mining processes to comply with GDPR as it relates to any EU customers."

Similarly, data cannot be repurposed for other uses, even though data repurposing is fairly common in big data applications. The Center of Data Innovation explained the immediate impact of this kind of regulation. The GDPR "will have a negative impact on the development and use of artificial intelligence (AI) in Europe, putting EU firms at a competitive disadvantage compared with their competitors in North America and Asia." But it will also have a significant impact on start-ups that might want to expand services or pivot to new services using their existing data.

All Data Processing Must Receive Consent

Under the new law, data subjects must consent affirmatively for data processors to use their data, and they can withdraw this consent at any time. Moreover, separate consents will have to be obtained for different processing activities. This requirement in particular has put the entire Internet ecosystem on notice.

Affirmative consent is also known as an opt-in privacy regime. Opt-in is frequently described as giving consumers more privacy protection, but opt-out regimes give an individual the same option to exit data processing without the added burdens. Indeed, most of the large companies already provide a method of opting out of certain data processing and collection. Setting the default by regulation simply biases consumer choices in a particular direction.

An opt-in privacy system imposes significant costs on the consumer, as an AAF analysis explained before. While this analysis focused on Internet service providers, the basic insight applies to all data processors:

Opt-in regimes present three big hurdles for consumers as decision makers. First, consumers have substantially less information about decisions they make. Before any additional service can be provided by the ISP, consumers will have to imagine all of the potential benefits, which will be difficult if not impossible. Second, consumers will think that that defaults are suggestions by the company. In other words, they will assume that it is a recommended action, even though they are mandated choices by the government. Lastly, these defaults will become the status quo. Any further change from this baseline will require significant effort by the ISP and will be understood by the decision maker as a trade-off, as psychologists have found.

The EU has already trekked down this path. In May 2011, it passed a Directive that gave individuals rights to refuse the use of cookies, requiring that everyone opt-in. An estimate found that this cookie regulation comes at a cost of nearly $2.3 billion per year. Other research confirm the cost. Because of the additional restrictions, display advertising decreased in efficacy by 65 percent as compared to display advertising in other countries. The decrease in effectiveness was especially pronounced for general content websites like news sites. Since startups and other content generators rely upon advertising revenue, this rule had the effect of cutting off the lifeblood of Internet companies.

Data Transparency, the Right To Portability, and the Right To Be Forgotten

The GDPR grants individuals a range of other rights, including the right to access their data, the right to know how their data is being processed, the right to data portability, and the right to be forgotten.

The GDPR gives data subjects "the right of access to personal data which have been collected concerning him

or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing." As an extensive of this right, new data breach notification requirements will take effect.

But, the implications of the right to know reach further than this innocuous description suggests on the surface. For example, many methods of big data analysis don't lend to easy explanation, so if companies are forced to explain what they are doing in plain text, then those algorithms will not be integrated in an effort to ensure easy explainability. Nick Wallace of the Center for Data Innovation explained the possible consequences of this provision: "Our fear is that this requirement in the GDPR, especially in the most significant circumstances, will either push companies to not use AI at all or to use substandard algorithms that are easier to explain but may produce less accurate and therefore potentially less fair decisions."

Data portability is another right outlined in the GDPR. In practice, the biggest social media platforms already allow for consumers to export their data. Some hope that the effect of this law will be more competition, but as another AAF analysis explained, there is no guarantee that this policy will achieve this goal. As the analysis explained, "Reassigning rights to data misses the fundamental point about data. It is not the mere presence of data that confers an advantage. Tech companies have to invest in their platforms, like any other asset."

Furthermore, individuals now have the right to erasure, more commonly known as the right to be forgotten. Under certain circumstances, search engines and other data processors must remove information about people. While some have praised this new right, civil libertarians, free speech activists and journalists especially have been concerned by the right, as it impedes the access of information. Not surprisingly, around a fifth of all requests to be delisted came from government officials and politicians.

The EU Could Level Severe Fines

The rights and obligations outlined above are just a taste of what companies face in nearly 200 pages of the regulation. But, what happens if a company fails to comply with the GDPR? For less serious offences, the fine is up to €10 million or two percent of the firm's global revenue, whichever is greater. For more serious offences, the fine is up to €20 million or four percent of the firm's global revenue, whichever is greater. Even if a company only has a small part of their total footprint in the EU, they are fined on the return of their entire company. For Google, a single fine for a serious offense could reach nearly $4.4 billion. Facebook faces nearly $1.6 billion in fine liability. But what distinguishes lesser offenses from more serious ones has yet to be defined. The European Data Protection Board (EDPB) has said they will offer direction on fines, but that direction is not available yet, leaving the first few cases to set precedent. In total, the fines could represent a potential extinction level event for liable companies.

Why Does The GDPR Matter In The United States?

The GDPR will have two kinds of impact, an indirect one and a direct one.

The indirect impact comes from the GDPR's influence on the development of other the legal systems in other countries. Transferring personal data out of the EU requires that the receiving countries have adequate levels of protection. Because the EU has 500 million people, smaller countries are adapting their regulatory standards to ensure companies in their borders have access to the European market. The effect is the exportation of EU privacy law elsewhere. Israel, New Zealand, South Africa, Argentina, Colombia, South Korea, and Bermuda have each taken up reforms to comply with the EU.

Christopher Kuner, co-chair of the Brussels Privacy Hub at the Vrije Universiteit Brussel, recently explained that "Data protection is a good example of Europe trying to extend its influence over other countries." He called it the Brussels Effect, but legal scholars describe this as long arm jurisdiction.

Thus, the direct impact for U.S. companies is that they may need to comply even if they don't technically have European operations. Even though the largest companies can absorb these costs, many have faced serious challenges in retooling their operations. WhatsApp has increased its minimum age to 16, and Snapchat has changed how its features work for its users who are under-16. Verve, a mobile marketing platform which relies heavily on location data, is exiting Europe altogether in response to the GDPR. Everyone is retooling their data processes completely to continue operating in the EU.

The Costs of Implementation

Companies are already feeling the compliance costs.

A PwC survey of 300 executives found that 88 percent of all companies are spending more than $1 million to become GDPR compliant, while 40 percent of companies are spending more than $10 million. Although the vast majority of U.S. firms have started the process of complying, only a quarter or so have completed it, suggesting that many companies will not be ready by the time the deadline rolls around on May 25th.

A McDermott-Ponemon survey on GDPR preparedness found that almost two-thirds of all companies say the regulation will "significantly change" their informational workflows. For the just over 50 percent of companies expecting to be ready for the changes, the average budget for getting to compliance tops $13 million, by their estimate. Among all the new requirements, this survey found that companies were struggling with the data-breach notification the most. The inability to comply with the notification requirement was cited by 68 percent of companies as posing the greatest risk because of the size of levied fines.

The two surveys share different perspectives when it comes to the correlation of firm size and compliance spending. McDermott-Ponemon's work suggest that mid-sized companies are the best prepared while both small and large companies are lagging. PwC finds that the largest companies are the best prepared for the new laws. Smaller companies and startups, however, will likely face the biggest burdens, since the GDPR offers no small-business exemption, unlike many other laws. Both surveys, however, reflect how demanding the GDPR is and the anxiety surrounding complying.

EU privacy laws have a history of being costly to the economy as a whole, as well. When the EU adopted the e-Privacy Directive in 2002, venture capital investment in online news, online advertising, and cloud computing dropped by between 58 to 75 percent. Thus, it should come as little surprise that members of the Fortune 500 will spend a combined $7.8 billion to come into compliance with the new European regulation. That's $7.8 billion *not* being put into innovation.

Conclusion

The GDPR is a dramatic change in privacy law. It creates sweeping procedural obligations, emboldened compliance monitoring, and massive data security requirements. While the law tries to grant people a plethora of rights over data, it comes at the expense of free speech, innovation, entrepreneurship, and business development.

For the soon-to-be regulated, or for those interested in the legal impacts of this law, the following links might be useful.

- The EU GDPR Portal
- The United Kingdom's data protection self assessment
- The Bird & Bird Guide to the General Data Protection Regulation
- Bloomberg Law's Analysis of "The Final European Union General Data Protection Regulation"