Stratecast | FROST & SULLIVAN

September 2017

Think the GDPR Will Only Impact the EU and UK? Think Again

Stratecast Analysis by

Jeff Cotrupe

Frost & Sullivan
7550 West Interstate 10, Suite 400
San Antonio, TX 78229
United States

Think the GDPR Will Only Impact the EU and UK? Think Again

Introduction

This document does not represent an exhaustive review of privacy, nor the General Data Protection Regulation (GDPR) passed by the European Commission (EC). Stratecast has addressed privacy in multiple reports in recent years, and again most recently with a four-part report series in 2017.[1] The intent of this brief treatise is to serve as a wakeup call to readers outside the European Union (EU) and the UK—many of whom appear to be marginally aware of the GDPR, or to know about it but believe their organizations are immune to its effects. That is pure fallacy, and this piece analyzes a select few real-world scenarios in which in the GDPR can impact us all, across world regions.

Scenario 1: Healthcare

From business travel to tourism to education to sports, people the world over have more reasons than ever to travel to other parts of the world. Should a traveler from the EU or the UK require medical attention, the facility where he or she seeks treatment is now subject to the GDPR. It is true that while the GDPR prohibits the processing of certain special categories of personal data, this is subject to certain exceptions, including genetic and health data. On the surface, that might appear to shield healthcare providers outside the EU or UK from the GDPR, but the devil is in the details. In order to be certain of GDPR compliance, health providers must ensure that their interaction with an EU or UK citizen qualifies as an exceptional circumstance as defined in the GDPR. The patient must first give explicit consent to the processing of his or her personal data. Then such processing must be deemed necessary to protect the patient's vital interests, and must be confirmed as essential to medical diagnosis; to the provision of health, treatment, or social care, including to enable the provider to practice preventive or occupational medicine; to assess an employee's ability to perform work; to enable management of health or social care systems and services; or to serve the public interest in terms of public health, such as an outbreak of a health threat across borders. The patient must be the one to grant explicit consent except in cases where he or she is physically or legally incapable of doing so.

Some of the GDPR's provisions as applicable to all industries including healthcare are not vastly different than those in the Health Insurance Portability and Accountability Act (HIPAA) enacted in the US in 1996. HIPAA states that health providers cannot share protected health information (PHI) without patient consent; must provide patients with their PHI within 30 days of patient request; and grants patients the legal right to request a correction if they feel something in their PHI is inaccurate. The biggest difference is that HIPAA was written to apply to healthcare services delivered in the US, with no attempt to enforce "legal portability"—the notion that HIPAA would travel with US citizens wherever they may roam—which is one of the cornerstones of the GDPR. Further, even while granting patients the right to contest parts of their PHI they feel are inaccurate, HIPAA does not go nearly as far as the Right to be Forgotten/Data Erasure provision of the

[1] This four-report Privacy series is as follows: Stratecast, *We Have Seen the Future of IT, and it is Big Data: Part 1 – Will IoT Privacy Issues Steal the Future?* (BDA 5-01, 30 June 2017); *We Have Seen the Future of IT, and it is Big Data: Part 2: A Blueprint for Privacy, in the IoT and Everywhere* (BDA 5-02, 7 July 2017); *Big Data is in Big Trouble, Starting in the EU: How the EU's GDPR Threatens to Destroy Big Data Initiatives and Business Opportunities, in the EU and Elsewhere* (BDA 5-03, 2 August 2017); and *Our Detailed Privacy Blueprint: What All Parties Should Be Doing Right Now to Protect the People and Organizations They Care About* (SPIE 2017-28, 11 August 2017); all available here

GDPR. This provision requires organizations in healthcare and every sector to comply with data erasure requests from EU citizens based not on whether some piece of information is accurate, but merely if an EU citizen does not like the information, e.g., if he or she finds it embarrassing.

Healthcare providers themselves are not the only ones affected by these provisions of the GDPR; laboratories, too, who support the providers with blood and other testing services are also subject to the law. The bottom line is that healthcare providers indeed are granted a special exception for data processing under the GDPR—along with a whole separate set of conditions to meet; and they must also remain current on any new regulatory changes on the part of EU member states, much as they strive to remain current on medical procedures.

Scenario 2: Banking and Financial Services

The implications of the GDPR on banks and financial services companies are broad, deep, and multifaceted; every provision of the GDPR can impact them. This point focuses on one simple scenario that may occur every day: a citizen of the EU or the UK traveling outside that region who wishes to access accounts via one of the global financial networks and withdraw money from an ATM. Once the traveler inserts a card into the ATM to begin the transaction, he or she begins providing information to the financial network in order to carry out the transaction. At that moment the bank housing the ATM is bound by all provisions of the GDPR with regard to obtaining explicit consent; protecting the user's data and being able to provide it to them upon request; offering data portability to enable them to bring it to another financial institution—or any company of any type—and, upon request, erasing all of the user's data from all of the bank's systems and databases.

That last point is a thorny one because there are bound to be conflicts between EU or UK citizen requests under the Right to Be Forgotten provision versus data retention requirements of a bank's home nation. For example, under the terms of the Bank Security Act in the US, banks must keep a detailed history of each checking and savings account for at least five years after the data is obtained.

In much the same way as the GDPR's provisions with regard to healthcare providers will also apply to the labs that perform testing for providers, the implications of the GDPR extend beyond banks and financial services companies to any ATM transaction that occurs, for example, in a grocery store checkout where an EU citizen wishes to get cash back from a transaction.

Scenario 3: e-Commerce

Moving from in-person transactions such as those described in Scenario 2 to e-commerce, one can envision an online shopper who finds amazon.co.uk does not have a particular piece of merchandise he wants or needs. So instead, he connects to US-based amazon.com—perhaps through one of the Amazon-integrated international shipping services that are springing up, such as flycrates.com. A bit differently than the bank example, the transaction must actually go through in order for data to be retained in the system, but once it is, Amazon becomes a data controller under the terms of the GDPR. Should the shopper raise a Right to Access data request, Amazon must be able to provide every instance, every place in the system, where the shopper's name and other personal details have been used, including in formulating algorithms at the core of its marketing systems. Amazon, and any provider thus selling to any citizen of the EU or UK, must know where and how the shopper's personal data is archived and secured, and must, upon request, be able to remove the data from every system across the enterprise—or provide the data to the consumer to comply with portability.

The impacts will also be felt by banks and others who are credit card issuers. Visa, MasterCard, or any firm that serves a customer who is an EU or UK citizen, regardless of where the firm is based, will, by virtue of the necessity to collect personal data, be subject to the GDPR.

An example of a service station in the US serving EU and UK citizens illustrates two sides of the coin with regard to the GDPR. The service station likely offers credit card payment at the pump for gasoline, and EU or UK citizens who rent cars while in the US may buy gas at the service station. Since those transactions are being handled by a third-party credit card processing service, the processor—and not the service station—must be concerned with GDPR compliance on those transactions. However, if an EU or UK citizen rents a car in the US and brings it to that service station for repairs; and the service station obtains and retains customer records other than simply for credit card payment; then the service station becomes subject to the GDPR.

Scenario 4: Any Organization Wishing to Analyze Data across World Regions

Any organization with customer and market data collected from multiple world regions, if it wants to run its business in any sort of unified fashion, must perform analysis on all of its data to assess performance against revenue targets and other KPIs; perform cost and flow analysis; and conduct trending analysis across the entire enterprise. To do so, the organization must commingle data from all locations. If any of that data has been collected about citizens of the EU or the UK, the organization is subject to the provisions of the GDPR. The "simple answer" propounded by many—to maintain a separate database for all personal data from citizens of the EU and the UK—addresses only one facet of a complex issue, data location, and not the implications of data usage. The truth is that data can be commingled, but granular data controls and capabilities must be imposed to prevent unauthorized users from seeing personal data on EU and UK citizens while performing analysis against that data. All organizations in all sectors, while not benefiting from the same exception treatment (nor having to meet the special requirements) as healthcare, will likewise have to remain vigilant about new laws enacted by individual EU member states that may go beyond the provisions of the GDPR. For under the German variant to the GDPR, any database containing personal data about citizens of Germany must be physically located in Germany.

Scenario 5: Any Organization that Stores Personal Content

Any organization that, knowingly or not, stores personal content of citizens of the EU or the UK, becomes subject to the GDPR. An example would be a citizen of the EU or UK who uses an online photo storage service. Should one of these users decide to terminate their use of the storage service, they will likely have agreed, when originally opting in to the service, to be responsible for removing their own images prior to shutting down their account. However, in keeping with the GDPR's provision regarding Right to be Forgotten/Data Erasure, the online storage provider is then responsible for deleting all personal data that was associated with their accounts, as well as any image content these users may have failed to delete themselves.

Stratecast
The Last Word

Each point analyzed in this report reinforces Stratecast's assertion that because the EU and the UK, combined, represent one of the world's most important financial centers—one that few companies operating globally could afford to ignore—**the EU's action with regard to the GDPR amounts to unilateral action that attempts to enact a *de facto* (or in truth, given the penalties specified in the GDPR, *de jure*) global standard for privacy at the behest of the leaders of a single world region.** Given that stark reality, we believe it would have been, to use a phrase we hear in British Premier League football (soccer), "a bit more sporting" of the EU to extend provisional voting rights, or at least the right to be heard, before the EC approved this legislation.

The good news is that Stratecast | Frost & Sullivan stands ready, with its breadth and depth of expertise in all privacy matters impacting all sectors worldwide, to offer expertise, guidance, and specific action items to help businesses survive and prosper despite the data usage constraints imposed by the GDPR.

Jeff Cotrupe

Industry Director – Big Data & Analytics

Stratecast | Frost & Sullivan

jeff.cotrupe@frost.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.