By Adam C. Johnson

Data Regulations: Power to the People

When was the last time you read the terms and conditions on a website or took a minute to learn how your data is being used and by whom? Chances are, you ignore the pre-opt-in checkboxes during e-commerce checkouts or you quickly scroll through the disclosures when you create a new account.

If you're like most people, you have little regard for who's collecting your data and how they're using it.

In recent months, you were probably inundated with emails about "changes to privacy policies" or "updates to terms and conditions." Did you read any of those changes?

What business leaders should know about GDPR, the sweeping regulation on consumer data rights that went into effect May 25, 2018, carrying stunning enforcement power.

Probably not; consumers have been conditioned to be apathetic toward most things data, at least until recently.

With smart, Wi-Fi-connected devices capturing an increasing amount of data, regulation has struggled to remain ahead of emerging technology—or to even remain current with it.

There's always been a tacit agreement about consumer privacy and free services from companies. If there's a free product or service (e.g., Gmail, Facebook, Twitter, Snapchat), it's likely that the company is collecting and using data from consumers who use their products.

Up until this point, however, consumers had only one option if they didn't like or agree with an existing policy or practice of the company: Quit using their services.

That's changed. We've entered a new era of privacy regulation called GDPR.

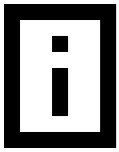
GDPR is the European Union's General Data Protection Regulation, which went into effect on May 25, 2018. It's considered the most comprehensive data regulation to date. GDPR requires businesses based in the EU and those outside the EU that offer services to EU citizens to treat data in a way that empowers consumers.

So, if data is the lifeblood of a company, then GDPR is a doctor-prescribed laboratory test of it.

The intent of GDPR, at its most granular level, is to increase transparency in how companies use consumer data. Transparency, as some policymakers assert, allows consumers the option to control their data and make more informed decisions about it.

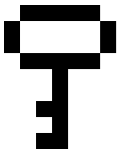
The regulation is somewhat ambiguous because it relays what items are required for compliance, but not how to meet those requirements, which was the unintentional result of four years of debate and a litany of compromises among EU policymakers. These debates continue.

Regardless, GDPR requires companies to provide consumers (aka data subjects) the following **RIGHTS:**



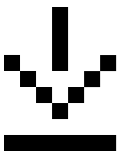
RIGHT TO BE INFORMED

Consumers have the right to know how their data is being used. This right often occurs at the time of consent, and the details of how consumer data is obtained, processed, stored, and transferred is typically relayed through a privacy policy near a call-to-action, in plain language.



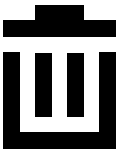
RIGHT TO ACCESS

Consumers have the right to view their data. GDPR provides provisions for what data a company should disclose. Generally, the provisions apply to any data that can be associated with a specific consumer. As a rule of thumb, companies aren't required to disclose data that is proprietary or is essential to their business models.



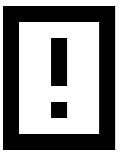
RIGHT TO PORT

Consumers have the right to download their data. This allows consumers the option of taking their data and using it with a different product or service.



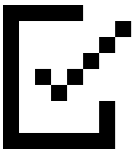
RIGHT TO ERASE

Consumers have the right to delete their data, formerly known as the "Right to be Forgotten." Because companies store and back up consumer data in multiple locations, the timing and type of deletion can be challenging for business leaders to work through, especially considering data localization laws.



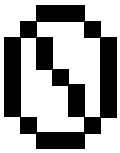
RIGHT TO OBJECT

Consumers have the right to object to the way a company uses their data or contest data processing practices. GDPR provides guidance on certain objections that require "compelling legitimate grounds," which legal counsel may be required to help business leaders navigate.



RIGHT TO RECTIFY

Consumers have the right to correct incorrect or incomplete data. Often, this is actioned through consumer-facing pages with self-editing functionality.



RIGHT TO RESTRICT

Consumers have the right to restrict how data is used by the company. Like the Right to Object, this right is difficult to put into action and may require in-depth discussions with legal counsel prior to developing functionality. It also may coincide with objections, rectifications, and erasures.

RIGHTS RELATING TO AUTOMATED DECISION-MAKING AND PROFILING

Consumers have the right to know whether a company uses their data for automated decision-making, profiling, and how, if desired, to request human intervention.

The cost of compliance and providing consumers these rights varies by company, but the penalties of violations can be severe. A GDPR violation could result in a fine up to 4 percent of annual global sales or around $24 million, whichever is greater.

It's evident that GDPR is forcing business leaders to have a conversation about digital privacy. In that conversation, business leaders should discuss how their companies obtain consent from consumers as well as how their companies collect, store, process, and share data—all items that are integral to GDPR compliance.

In doing so, most leaders will find it necessary to reevaluate their data governance processes, legal disclaimers, incident response, and data breach notification practices. And, in some instances, they may find it necessary to adjust their business practices.

For example, they might stop using default opt-ins for marketing subscription preferences or stop guerilla marketing campaigns altogether. Neither is considered GDPR compliant.

Finally, U.S.-based companies with a physical or web presence in the EU are required to treat data collected in the EU according to GDPR standards. But having realized that public sentiment toward data privacy is changing, companies should consider treating all consumer data according to this standard—regardless of where or whose data is collected—providing the same functionality of GDPR to all "in spirit."

CONSUMERS HAD ONLY ONE OPTION IF THEY DIDN'T LIKE OR AGREE WITH AN EXISTING POLICY OR PRACTICE OF THE COMPANY: QUIT USING THEIR SERVICES.

Adam C. Johnson
adam.johnson@jabian.com