All About the GDPR

While deregulation has been a stateside trend over the past decade, the 28 members of the European Union are gearing up for a massive increase in regulations around data privacy in the form of the General Data Protection Regulation (GDPR) – and this regulation will make a splash across the pond as well.

Briefly, virtually all personal information will be considered private and protected under these new rules, serving up a much more comprehensive approach than the US's piecemeal protections of medical and financial data.

But what do these new rules mean – if anything – for US businesses?

The short answer: Plenty. Maybe. It depends.

The long answer requires some context and is worth taking the time to understand. And most providers are already making big strides to be ready for launch in May.

Internet privacy: The early years

The GDPR, set to go into effect on May 25, 2018, is the product of four years of debate and preparation – but its roots trace back more than two decades to the infancy of the internet, when the EU first began protecting data. The GDPR will replace a 1995 regulation that was put into place when Netscape ruled the web, well before data giants like Google and Amazon began to flex their marketing muscles. Since then, the digital landscape has changed – and so has the way businesses utilize data. The EU is hoping to keep up with those data giants and those changes, ensuring its citizens can be confident in their privacy and security.

Like its predecessor, the GDPR is built on the premise that private information actually is, or should be, private and that individuals have rights surrounding this data. In fact, among the first words of the regulation are "data protection as a fundamental right." As to what comprises personal data, the GDPR is very specific:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier 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…"

How is the GDPR different from before?

As for the big differences between previous EU privacy standards and the GDPR, there are three primary areas of expansion:

- **Territorial scope.** This is arguably the biggest upgrade in the GDPR, giving it jurisdiction over all companies processing the personal data of individuals in the EU, whether the company is based in an EU nation or not. It covers all activities relating to the offering of goods and services to EU citizens and the monitoring of behavior that takes place in the EU. Pre-GDPR, territorial issues were fairly ambiguous, resulting in numerous complex legal cases.
- **Businesses wanting to use EU citizens' data need to obtain consent in a clear and accessible way.** Requesting consent via convoluted legalese or extremely fine print is not acceptable. Equally important, the entity seeking to use the data must make it as easy to withdraw consent as it is to grant it.
- **There are various degrees of penalties, some of which are significant.** For serious infringements, including failure to acquire consent, organizations in violation of the GDPR can be fined up to 4 percent of their annual global turnover or €20 million, whichever is greater. Lesser violations, such as insufficient record keeping can face a lesser, but still hefty, fine of 2 percent.

How does the GDPR differ from US privacy regulations?

The GDPR stands apart from the American approach to information privacy in its comprehensive nature. Its policies are sweeping, whereas the US has taken an ad hoc or sectoral approach. The US is given to the fairly sporadic adoption of industry-specific and (sometimes weirdly) niche regulations. For example, the Video Privacy Protection Act specifically forbade the release of lists of customers' video rentals from Blockbuster and so forth. Sounds outdated, but the VPPA has actually evolved to impact the way Netflix and Facebook handle information around video content. But even though it's come a long way from its analog origins, one can argue that it is hardly a comprehensive way to manage data privacy.

We also have the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Information Data Security Standards (PCI DSS), and countless other piecemeal bits of privacy. It's complicated. The EU's new standard, however, isn't complicated, at least not within the EU. It

doesn’t matter if the data is regarding your healthcare, your credit card, your video rentals, your DNA, your dating profile or anything else. If it’s your personal data, it’s protected under the new regulation. And the businesses that require personal data to do business with you must take the proper steps to acquire it, store it, process it and secure it. End of story.

How will this affect my US business?

Marketing in the digital age is all about data, so yes, the GDPR will complicate the job of marketers and can potentially jeopardize your business if you’re not careful. For example, if your social marketing channel happens to drift overseas and get “liked” by a Slovenian user, you won’t have to cough up €20 million. But if you create a website ending in .si to actively engage with that Slovenian market—or .uk or .es or any other EU nation suffix — or if you start accepting euros or pounds sterling or Danish Krones, the GDPR will likely apply to the data involved in those sites and transactions.

Companies that handle massive amounts of data, like Facebook, Netflix and Amazon, will have an obvious heavy lift to ensure they’re taking proper measures with individuals in the EU. But for everyone else, adopting the GDPR as best practices is a smart way to stay protected at home or abroad.

The good news is that many data-focused platforms are already providing compliance-focused features, many of which will overlap with the GDPR’s requirements. Marketing, email and data-tracking providers like Google, HubSpot and CallTrackingMetrics, for example, already have built-in functionality that allows users to maintain compliance with regulations like HIPAA and PCI. These tools, along with countless others, will also provide the coverage you need to meet GDPR compliance, as long as you are also fulfilling your

commitments to the overall philosophy of the regulation through initiatives like DPAs and policy revisions.

Serving up trust and customer experience

In most cases, the tools already exist or will exist to keep you compliant, but it’s up to you to follow best practices. Marketers need to be aware that the data they collect must have been acquired with consent, and it must be relevant to a specific purpose. If you’re holding a sweepstakes, for instance, the data you collect must be used for that purpose and that purpose alone. To maintain GDPR compliance, marketing databases will need constant scrubbing and/or additional consent – a wakeup call for marketers who have been building large, all-encompassing lists based on any and all contact data.

Regardless of a little extra work, the raison d’être of the GDPR remains solid: A thriving economy in this new digital,

data-driven world requires participants who are confident of their privacy – who feel their personal data belongs to them and trust the businesses they interact with. While this might feel like a major undertaking for individual US marketers, it's positive news for the industry as a whole. The GDPR is pushing us away from list-buying and other spammy practices and toward a better customer experience – which should be the ultimate goal of every marketer.

Opinions expressed in this article are those of the guest author and not necessarily Search Engine Land. Staff authors are listed here.

About The Author

CallTrackingMetrics provides thousands of businesses the tools they need to track, manage and optimize phone calls to increase conversions and scale for growth, worldwide. From understanding which advertising campaigns are driving phone calls to advanced routing and call management, we arm businesses and agencies with the tools to transform communication into powerful intelligence.
http://feeds.searchengineland.com/~r/searchengineland/~3/4jkhvjh-9GM/all-about-the-gdpr-294664