THE VERGE

WEB REPORT FEATURED VIDEOS

66

Everything you need to know about GDPR

GDPR gives companies a new set of rules for sharing data online

By Russell Brandom | @russellbrandom | Updated May 25, 2018, 9:52am EDT

Illustrations by William Joel

May 25th marks the first day of enforcement for Europe's General Data Protection Regulation, otherwise known as GDPR, a set of rules that could fundamentally flip the relationship between massive tech companies that gather data, and the users they gather it from.

Not everyone is ready for GDPR, but companies from Google to Slack have been quietly updating their terms, rewriting contracts, and rolling out new personal data tools in preparation for the massive shift in the legal landscape. So far, it's mostly been a problem for legal departments, but as policy changes and contract fights go public, it's started affecting the average web user, too.

Still, for many on the internet, GDPR remains a black box of legalese and obscure policy. Here's what you need to know about it.

WHAT IS THE GDPR?

The General Data Protection Regulation is a rule passed by the European Union in 2016, setting new rules for how companies manage and share personal data. In theory, the GDPR only applies to EU citizens' data, but the global nature of the internet means that nearly every online service is affected, and the regulation has already resulted in significant changes for US users as companies scramble to adapt.

Much of the GDPR builds on rules set by earlier EU privacy measures like the Privacy Shield and Data Protection

THE NEW RULES GO INTO EFFECT

Directive, but it expands on those measures in two crucial ways. First, the GDPR sets a higher bar for obtaining personal data than we've ever seen on the internet before. By default, any time a company collects personal data on an EU citizen, it will need explicit and informed consent from that person. Users also need a way to revoke that consent, and they can request all the data a company has from them as a way to verify that consent. It's a lot stronger than existing requirements, and it explicitly extends to companies based outside the EU. For an industry that's used to collecting and sharing data with little to no restriction, that means rewriting the rules of how ads are targeted online.

ON MAY 25TH

Second, the GDPR's penalties are severe enough to get the entire industry's attention. Maximum fines per violation are set at 4 percent of a company's global turnover (or $20 million, whichever is larger). That's a lot more than the fines allowed by the Data Protection Directive, and it signals how serious the EU is taking data privacy. Google and Facebook could withstand a fine like that (they have before), but it would be enough to sink a smaller firm. If the new consent rules ask companies to reshape their data policies, the proposed fines give them the motivation to make it happen.

Most importantly, the GDPR gives companies a hard deadline: the new rules go into effect on May 25th, 2018 — so if you're not following the rules by now, you're in trouble. The result has been a mad dash to adapt current practices to the new rules and avoid one of those crushing fines.

WHAT'S GOING TO CHANGE?

The most visible and immediate changes are coming in Terms of Service and other warnings. The GDPR's idea of consent requires a lot more than previous regulations, which means companies will be asking permission to collect your data a lot more often. In concrete terms, that means a lot more "click to proceed" boxes, although the transparency requirements mean the text inside may be a little clearer than you're used to.

There will also be more opportunities to download all the data a company has on you, something companies are already

THE MOST IMPORTANT

starting to roll out. Services like Google Takeout have existed for a while, and smaller services like Slack are starting to roll out similar options to satisfy the GDPR's data portability requirements. That helps in two ways: it lets you check what companies are collecting, and it could help unwind platform dominance by letting you transfer data between networks. If you want a way to export your Facebook messages to Ello, the new portability requirements will ensure there's a way to do it.

CHANGES WILL BE HAPPENING BEHIND THE SCENES

The most important changes will be happening behind the scenes. The GDPR also sets rules for how companies share data after it's been collected, which means companies have to rethink how they approach analytics, logins, and, above all, advertising. A single site could easily have 20 ad-targeting partners, often invisible to the person whose data is being shared. But the GDPR adds complex new requirements for any company that gets user data secondhand, requiring a lot more transparency on what a company is doing with your data. As a result, all of those partners have to be brought into the open, and their contracts have to be rewritten to comply with the GDPR. That means unearthing a notoriously messy system that's been built on the idea that there's no cost to sharing data.

Rewriting those contracts isn't as simple as adding some extra "I Agree" dialogs. There are hard political issues in play, like whether publishers will retain control of their audience data or whether ad networks like Google can piggyback on publishers' consent forms. When I talked to Shannon Yavorsky, a lawyer who has been following the GDPR requirements at Venable, she said clients were particularly stymied by the question of who would be liable if data was breached from a sharing partner. "I get asked all the time, what's the market standard?" Yavorsky says. "We just don't know. There haven't been any penalties, so we don't know what the enforcement is going to look like." There's no obvious fix to any of those issues, and the underlying disagreements will rage on long beyond the May deadline.

WILL THIS ACTUALLY MAKE ONLINE DATA

COLLECTION LESS CREEPY AND INVASIVE?

It's too early to say. We know roughly what compliance looks like, but we still don't know what enforcement will look like or how aggressive the EU regulators will be. The simplest takeaway is that breaches will get a lot more costly, and that cost will be spread a lot further through the network. It will get more expensive to share user data, and sites will probably try to make do with fewer partners, which would certainly be a win from a privacy perspective. Regulations like this tend to hit small companies the hardest, so the GDPR might also tip the scales even further toward big players like Google and Facebook, even as the overall pool of data shrinks.

The rule could also create a divide between the European Union and the rest of the internet. So far, most companies have aimed for a single set of privacy rules for all users, which is why so many US users are noticing new privacy features and terms of service. But in many cases, it's still easier to split off EU data, which could result in European users seeing a meaningfully different internet from the rest of the world.

On the other hand, it would be hard to make data collection *more* creepy at this point. So much of the internet is based on the free exchange of user data, especially the gnarly hairball that is the targeted advertising industry. That has real political consequences: the NSA can use the same system to track users across the web, and political firms like Cambridge Analytica can use it to quietly single out particular subgroups. We've spent the last 15 years thinking of lucrative things to do with that data, on the assumption that it would always be freely shareable. The GDPR is starting to roll it back, but the most profound changes will take years to play out, potentially reshaping the web as we know it.

Update May 25th, 9:49AM ET: *This story has been updated to reflect the launch of GDPR.*