

A hand-drawn infographic with various notes and diagrams. It includes a central banner that says 'The GDPR comes into force on 25 May 2018. The aim is to strengthen data protection and privacy for individuals in the EU.' To the right, there's a section titled 'Create Data Protection Officer Role (D.P.O.)' with a note: 'This person will be responsible for overseeing data protection, privacy and GDPR compliance. All public authorities (Police, L.A., Government) MUST have a D.P.O.' Below that, it says 'GDPR Extends Beyond the EU'. On the left, there are notes about 'Right to be Forgotten' and 'Data Portability'. At the bottom, there's a section titled 'RANGE OF DATA'.

Dissecting the General Data Protection Reg...

By Rich Cefola on May 22, 2018

In a few short days, the full brunt of the European Union (EU) General Data Protection Regulation (GDPR) will be enforced. The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

It is to be the broadest accepted and enforced data privacy policy protecting "personal data." According to the European Commission, "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address." A major focus of GDPR is on conditions of consent which have been strengthened. So, companies will not be able to use vague or confusing statements to get you to agree to give them data. Firms won't be able to bundle consent for different things together either. Akin to what happened in Facebook's now infamous Cambridge Analytica scandal of exposing information.

Will it make online data collection less creepy?

It's too early to say. The compliance side is in place, but the enforcement will tell the story of how aggressive the EU regulators will be. The easiest takeaway is that breaches will get a lot costlier, and that cost will be spread a lot further through the network. The price will certainly go up on sharing 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.

It would be hard to make data collection *creepier* 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](#). 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.

So, until next time, as far as data protection and consent goes - know that it is out there, we need to stay out in front of this. Even in the government space, this could have far reaching implications.