Your Guide to the GDPR - General Data Protection Regulation

Author : Cat

Date : May 1, 2018

What is the GDPR?

The *General Data Protection Regulation* is a framework of legal guidelines for collection and processing of personal info of individuals within the European Union. Or, in short, it's new rules that companies need to follow to collect and protect a user's data. As of May 25th, 2018, any company, group, or individual, that handles European data must comply with GDPR. This goes for massive players like Google down to bloggers who collect email address for their newsletter.

Four terms to understand:

Personal Data - any identifying information . This includes submitted information such as your name, email, SIN, address, phone number, biometrics, or account numbers. It also includes information that could be used to identify you indirectly such as location data.

Data Subject - simply put it is the user or the person who is identified by the information.

Data Controller - the person or company who determines the purpose and use of the collected data.

Data Processor - the person or company who processes the data. This includes analytics, marketing, as well as storage such as cloud services.

The *controller* and *processor* can be the same or separate. For example, I collect email addresses for my newsletter. That makes me the *controller*. I can chose to store these addresses on my computer, that makes me the *processor.* Alternatively I can chose to store them in Mailchimp, which is a newsletter app, or perhaps on a document in Google Drive, which is the cloud. Now I have chosen an outside *processor*. As the *controller*, I am responsible for GDPR compliance for both me and my chosen *processor.*

New Security and Privacy Features

The full regulation is over 100 printed pages long. It includes your rights as a *data subject* as well as regulations around how *collectors and processors* are required to protect your data.

There are the five main pillars:

Right to be forgotten - This is the most talked about and least understood. It is the right for a user to retract their data from storage or processing, from any company at any time. When the Cambridge Analytica scandal broke with Facebook, people wanted to delete their accounts but the data was still out there. This ruling would have forced both Facebook and Cambridge Analytica to delete the data they had on any qualifying individual that requested it. This is NOT an opportunity to have unflattering articles or reviews removed. The rule allows for personal mentions if they fall under freedom of expression, public interest, public health, or research.

Right of access - As a *data subject*, this is your right to ask about the purpose for the collected data, the *processors* involved, and even if the data is being manipulated with artificial intelligence or machine learning. All these answers *should* be covered in the new consent request (see below).

Right of restricton of processing - You know those pesky ads that follow you from one website to another? That's called direct marketing. The *restriction of processing* means you can indicate specifically that you do not want your data used in direct marketing campaigns.

Consent - For all data collection, the *data subject* has to have the ability to both opt in AND withdraw consent. *Collectors* also have to present the information to support *right of access.* I like to break these down as the 5 Ws:

- WHO - Details of the recipients of the data including links to the *controller*
- WHAT - List of the data being collected
- WHY - Reason for the collection
- WHEN - The duration for which the data will be retained

- WHERE - Clear links provided so user knows where to go to withdraw requests

Example: for my newsletter sign-up, it will need to say "Binary Tattoo [WHO] will be collecting your name and email address [WHAT] via Mailchimp [WHO] for the purposes of our newsletter only [WHY]. We will maintain this record indefinitely [WHEN]. You may opt out any time at this *link* [WHERE]*."*

Reporting of Data Breaches - In terms of protection of data, this is a big one. In the past there was NO regulation that a company had to report a breach. Uber took 6 months to report their 2018 data breach. Now compliant companies have to report any breaches within 72 hours of their knowledge.

For Individuals

Technically the GDPR only applies to citizens in the European Union. In fact, the UK (post-Brexit) doesn't even fall under these rules though they do support a *Data Protection Bill*, which is similar. As a Canadian I am not entitled to *Right to Be Forgotten* under current North American rules. That said, it is far easier for companies, especially bigger ones, to alter their rules and terms globally than it is to determine who is or is not a citizen of the EU, so we should expect to see changes across many of the services we use. Check the links below for the new terms and service agreements.

For Businesses and Corporations

Any organization that "processes or stores large amounts of personal data, whether for employees, individuals outside the organization, or both" is required to designate a **Data Protection Officer.** That person is responsible for ensuring compliance of GDPR.

If a company is caught in non-compliance then they face a fine. Depending on the infraction, a tier 1 offence results in a fine of the higher of 2% of the company's world wide gross revenue or 10 million euros. A tier 2 offence is the higher of 4% of global revenue or 20 million euros. As an example, when Equifax was breached in 2017 they suffered no penalties. Had GDPR been in place they would have owed 67 million dollars in fines.

Every applicable company needs to run a **DPIA,** or *Data Protection Impact Assessment,* that includes an explanation why they are collecting the data requested, an assessment of risks to the rights and freedoms of data subjects, and documented proposed measures for safety and security of the collection.

For Bloggers, Charities, Clubs and Everyone else!

Unfortunately even small businesses, groups, not-for-profits, and charities fall under these new regulations. If you run or are part of a group that collects information (newsletters, databases, list serves, forums, etc.) then this could apply to you. Fortunately most of the individual tools that small business uses, like cloud servers, Newsletters, and CRMs, are updating their terms to comply.

What you should do:

- Make a list of all of the software and services you use (good to have this anyway)
- Consider each one for data collection, storage, and processing
- For those that do, type the name of the service and 'GDPR' in to Google for instructions

Loads of Links

After having gone through multiple sites, here several you may find useful:

- The official GDPR site
- The entire GDPR brown down nicely by links
- The GDPR broken down by chapter and in plain english
- Facebook group: GDPR for entrepreneurs - as written by a lawyer

Actions for Businesses that Collect Data

- Getting consent in Google For Business - as collectors. Includes ads, apps, sites
- Google's G-suite and Cloud Agreements - as processors
- AWS GDPR site
- Dropbox
- Rules for Email Marketers
- Mailchimp's New Consent Collection
- Facebook for Business
- LinkedIn for Business - includes marketing, sales, developers

New Individual Terms and Services for Networks

- Facebook
- Instagram (now combined with Facebook)
- Twitter
- LinkedIn - link for their new terms, coming soon.

If you have any questions or find something we've missed let us know!