STRENGTHEN AND UNIFY DATA PROTECTION FOR ALL INDIVIDUALS WITHIN THE EUROPEAN UNION

PIVOT · PATH
MARKETING STRATEGISTS AND CREATIVE STORYTELLERS.

Five Big Questions Related to GDPR

First things first. We're not lawyers, and what follows does not constitute legal advice. We have a vested interest in the success of our partnership and want to provide information to collectively aid us through this process. If you want true legal advice, we advise you seek out private counsel. That being said, let's get you prepared for the General Data Protection Regulation (GDPR) that went into effect May 25, 2018.

Here are five big questions related to GDPR:

1. What is GDPR?
2. Does it affect our company or organization?
3. How does this change the way we collect and store data?
4. How does this change the way we communicate and market?
5. How do we get started?

WHAT IS GDPR?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The European Union currently has data protection regulation that determines how personal information can be used by companies, the government, and other organizations.

GDPR changes the definition of personal information and how data is obtained and used. Within GDPR, there are 99 articles setting out the rights of individuals to have easier access to the information data companies collect about them, determinations of fines related to non-compliance, and responsibilities for obtaining consent and usage of personal information. This law provides greater transparency, enhanced rights for EU citizens, and increased accountability.

DOES IT AFFECT OUR COMPANY OR ORGANIZATION?

GDPR regulations apply to any company that processes EU consumer data, no matter where the company resides or where the servers that collect the data are located. These provisions promote accountability and governance. These measures were designed to minimize the risk of breaches and uphold the protection of personal data.

Compliance for GDPR does not lay at just the feet of marketers, but in all processes of data storage, collection and usage, and thus should become a boardroom topic if it has not already. Additionally, companies that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data may have to designate a data protection officer (DPO).

That may seem like a lot of change, but if you're already in compliance with current laws, the GDPR should just be a step up. Here's an excerpt from a blog from the Information Commissioner's Office (ICO), written by Deputy Commissioner for Policy, Steve Wood:

The new regime is an evolution in data protection, not a revolution. Let's start off by being totally up front here. Any regulation has some sort of impact on an organization's resources. That's unavoidable and GDPR is no different to any other new legislation in that respect. But thinking about burden indicates the wrong mindset to preparing for GDPR compliance.

What must be recognized is that GDPR is an evolution in data protection, not a total revolution. It demands more of organizations in terms of accountability for their use of personal data and enhances the existing rights of individuals. GDPR is building on foundations already in place for the last 20 years.

If you are already complying with the terms of the Data Protection Act, and have an effective data governance program in place, then you are already well on the way to being ready for GDPR. Our GDPR overview and 12 steps to take now documents explain where there is continuity, what's new and how to plan.

Many of the fundamentals remain the same and have been known about for a long time. Fairness, transparency, accuracy, security, minimization and respect for the rights of the individual whose data you want to process – these are all things you should already be doing with data and GDPR seeks only to build on those principles.

That doesn't mean there's any room for complacency. There are new provisions to comply with and organizations should start making preparations now, if they haven't done so already. But by and large, the new GDPR regime represents a step change, rather than a leap into the unknown.

HOW DOES THIS CHANGE THE WAY WE COLLECT AND STORE DATA?

LAWFULNESS

Not everyone that handles personal data of individuals is the same, and GDPR regulation falls within two main categories: controller and processor. A controller is an entity that decides the purpose and manner in which personal data will be used. This is your role. A processor is a person (or team) that processes data on behalf of the controller; and includes obtaining, recording, adapting or holding personal data. GDPR requirements are different for each. In addition, the controller is responsible for, and must be able to demonstrate, compliance with GDPR principles.

Bottom line: *for data processing to be lawful under GDPR, companies need to identify a lawful basis for processing personal data, and be able to document this.*

THE RIGHTS OF INDIVIDUALS

The GDPR was established to maintain higher standards when it comes to personal information that provides individuals with the following rights:

1. ***The right to be informed*** *[The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice.]*

2. ***The right of access*** *[Individuals have the right to access their personal data and supplementary information.]*

3. ***The right to rectification*** *[The GDPR gives individuals the right to have personal data rectified if data is inaccurate or incomplete.]*

4. ***The right to erase*** *[The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.]*

5. ***The right to restrict processing*** *[Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.]*

6 ***The right to data portability*** *[The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.]*

7 ***The right to object*** *[Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.]*

8 ***The rights in relation to automated decision making and profiling.*** *[The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.]*

9 ***The right to withdraw consent.*** *[Controllers must inform subjects of the **right to withdraw** before **consent** is given. Once **consent** is **withdrawn**, data subjects have the **right** to have their personal data erased and no longer used for processing.]*

10 ***The right of data protection.*** *[Under the GDPR, you have a general obligation to implement technical and organizational measures to show that you have considered and integrated data protection into your processing activities.]*

CONSENT

GDPR sets a high standard for consent, which puts the individual in control of their data and how it is used—the biggest change will be in your processes for collecting consent.

According to ICO's Guide to the GDPR, companies need to follow specific guidelines to obtain, record and manage consent:

- Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand.
- Include the name of your organization and any third party controllers who will be relying on the consent, why you want the data, what you will do with it, and the right to withdraw consent at any time.
- You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or default settings.

- Wherever possible, give granular options to consent separately to different purposes and different types of processing.
- Keep records to evidence consent—who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.
- Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

From these requirements, a clearly written privacy policy is a must, along with forms designed to inform while gaining consent, and self-subscription management pages for subscribers to update their information (or remove it) should be available.

TRANSPARENCY, ACCOUNTABILITY AND GOVERNANCE

GDPR's requirements for accountability and governance most certainly will require some businesses to enhance their structure in capturing and holding personal data, but truly these measures are simply meant to champion the importance of personal data privacy and minimize security risks. So not only do you have to put specific reviews and measures into place, but also have documentation of such to prove compliance should that ever be needed.

HOW DOES THIS CHANGE THE WAY WE COMMUNICATE AND MARKET?

As long as you don't get bogged down by the hype (remember Y2K), most pure marketers will understand that GDPR is actually a blessing. It forces us to be responsible and better marketers—and to provide our subscribers with exactly what they want. And that's the way we all should be marketing. So think of this as a new (albeit required) goal to only communicate with those who want to hear from us, be ever-present in true permission based marketing and to have all data in order which can only build trust and loyalty with subscribers.

HOW DO WE GET STARTED?

Having a full understanding of GDPR is important, as it may impact a number of facets of your business practices. The place to start is in education, and while there are a myriad of articles and resources on the net, we find the information from the Information Commissioner's Office—the UK's independent authority set up to uphold information rights in the public interest—to be the most credible.

Check out these ICO resources to get started
(Click the titles below to direct you to guide documents)

- **Guide to the GDPR**
- **GDPR: 12 Steps to Take Now**
  Getting Ready for the GDPR Checklist:
  - ***For data controllers***
  - ***For data processors***
- **GDPR Checklist**