GPDR: what it is, what is changing, what you need to do

The GDPR is the new European regulation on privacy that will apply to all European citizens and companies. Are you already complying? Find out what you need to do.

If it's about privacy, it's about GDPR: this acronym stands for General Data Protection Regulation. It's a European norm, Regulation UE 2016/679, issued on April 27, 2016 which will come into effect on May 25, 2018.

"*Does this affect me? Does it only affect big companies, or small businesses too? Does it affect freelancers? Does this affect me, if all I have is a blog?*" These are the questions you're surely asking. The GDPR applies to anybody who handles personal data: so if you have an e-commerce website, or a website that collects e-mails for a newsletter, or even if you sometimes need to ask for a client's phone number as part of your customer service, this regulation also applies to you.

In this post, you will get to know it better and learn what to do and where to find official and useful sources.

We will discuss:

- The GDPR's ration legis: we'll understand its purpose
- In concrete terms: what to do
- Sanctions: what happens to those who don't follow the GDPR
- To Do List: the GDPR in 5 points
- Useful resources

Happy reading!

Behind every law, there's a reason: experts call this reason the "ratio legis". Understanding the ratio legis is useful for putting all the changes and improvements that will be asked of you into the right context... and will help make these changes less of a headache.

The "charter of the data economy"

The "ratio legis", the reason behind the GDPR, can be summed up as follows: data is and always will be the "raw material" that powers a new economy based on the extended use of data as well as a strategic element in the development of innovative products and services. The GDPR is the charter for this new economy. The goal of the GDPR is to knock down national jurisdiction barriers and to create a set of shared rules for handling personal data throughout the European Union; rules that apply to anybody who handles data in Europe (including "American Giants" like Google and Facebook).

From formal compliance to a corporate process

Before the GDPR, privacy was often considered an secondary element and a purely formal requirement ("to avoide a fine from the Privacy Authority"). With the GDPR, however, privacy becomes a fully developed corporate process, which is integrated into the business plan of all companies, whether they are large, medium-sized, small, or micro-businesses.

Principle of minimization

As little data as possible, only useful data. No data may be collected beyond that data for which explicit consent is requested: the days of, "you never know, this may be useful someday," are over. Keep this in mind when you pick the fields to include in a contact form, or at any other point in which visitors to your website may leave behind data.

Privacy by design

The protection of personal data must be guaranteed from the first planning stages of a project through the entire data handling lifecycle.

Privacy by default

Privacy becomes a requirement; it is no longer secondary, but rather the "default" in handling information. This requires planning an entire series of technical data protection measures, such as pseudonymisation, a process which prevents data from being traced back to a specific person.

What concrete steps do I need to take to comply with the GDPR?

Now that we understand the premise, here is a summary of the changes which the GDPR requires you to make in the way you handle the personal data of your clients or prospects.

This statement is no longer just a formality either: its goal is to make sure the reader knows which data will be processed, and more generally, what is involved. That is why the statement needs to be brief, transparent, and always accessible and understandable to all, including minors. The language must be clear and effective, and the user can also be informed verbally (but only if they requet it, and once their identity is verified), and the statement can be made gradually, one piece of information at a time (layered statement). In addition to written text, standard icons may be used to increase comphrehension.

Consent: saying yes to awareness.

Consent must be positive and inequivocal: tacit or passive consent is no longer acceptable. Furthermore, consent must be specifically given for each aspect of data handling: if you collect data – for example, first and last name and e-mail address – in order to issue a quote, this is the first level of service for which you must obtain consent. If, as is likely, this data is added to a database which you intend to use for commercial actions – for example, to tell people about a Christmas sale – this constitutes a second level of data handling, which you must explicitly list in the disclosure.

One example of a positive and inequivocal action is when the user clicks to continue navigating the website after having viewed a banner disclosing the use of cookies.

Managing privacy risks: the DPIA is born.

The GDPR mandates the use of a Data Protection Impact Assessment (DPIA), a document for evaluating the impact of data protection. With the DPIA, privacy management becomes fully integrated into business management methods and intersects with safety management (which, in Italy, is regulated via legislative decree 81/2008), which hinges on concepts of risk and risk prevention management.

The DPIA document implements the privacy risk management process in 3 phases:

- privacy risk analysis
- compiling a list of the current management system's weaknesses with regards to these risks (gap list)
- defining an intervention plan to minimize these risks (action plan)

What to do when things "go wrong": data breach notification.

If a data breach is confirmed, meaning a security failure or gap occurred and caused data to be lost, destroyed, modified, disclosed, or made accessible to unauthorized individuals, a data breach notification must be issued to the affected parties immediately as well as to the Privacy Authority within 72 hours of the breach. The notification must contain certain information, including:

- Name and contact information of the Data Protection Officer or the person to contact for more information.
- Description of the breach
- Description of the measures adopted or to be adopted to remedy the data breach, and its potential consequences for the affected parties.

The obligation (which applies to certain companies and certain types of data) to preventively inform the Privacy Authority has been rescinded and replaced by a new document, the data processing register. One could say this is "phase 2" of privacy management, which follows the impact evaluation and is to be used as an internal planning tool. It is not mandatory for companies with less than 250 employees, unless "the data handling they carry out

- could present a risk for the rights and liberties of the concerned parties,
- this data handling is more than occasional,
- or it includes the handling of particular categories of data (Ed: known as sensitive data.),
- or personal data relating to criminal convictions and crimes (Ed: known as judicial data)"

This document must also contain an entire series of data: at the bottom of this post, we recommend a service for creating a datat processing register and managing your privacy information.

The DPO (Data Privacy Officer) is born.

Implementing the GDPR doesn't just mean having the documents ready, it also requires the right positions in the company. The GDPR is very clear in this regard: the positions we are currently familiar with remain, meaning the data controller, data supervisor, and the person in charge of data processing, with the addition of a person in charge of personal data handling, namely the Data Privacy Officer or DPO, who serves as an independent internal auditor who has legal and IT skills, as well as spending autonomy and decision-making auhtority. As in the case of the data processing register, not every company will require a DPO; only those which handle a certain amount of personal data, and do so more than occassionally, or which handle sensitive or judicial data, or which are public entities.

What happens to those who don't follow the GDPR?

Penalties are pretty substantial: they can result in up **4% of sales up to a maximum of 20 million Europ**.

What do I need to do? A 5-point GDPR to-do list

First: verify your website's privacy statement.
Make sure it contains all necessary elements (below, you'll find a tool that can help you manage this). Then read it, or have somebody else read it, and ask: is this understandable? Is anything not clear?

Second: map out all the points at which you collect user information.

Third: describe the way in which you actually handle data.

Start from the moment it is collected and continue until how it is stored. To do this, here is a set of guiding questions.

- What tool or service do you use to collect e-mail addresses? What kind of data handling do they use? Where does this data end up once you've collected it?
- Once you've collected data, where do you store all the data you handle? On what kind of database? What server hosts this database? Is the service provider GDPR-compliant? And so on.
- Who analyzes the data (for example, who compiles e-mail addresses for promotional activities)?

Fourth: use all this information to draw up the DPIA, the risk impact analysis.

On the Privacy Authority's website, you'll find a software to help you write this up. If you're unsure, consult an expert.

Fifth: review, change, implement.

With the help of an expert, review your privacy statement and all the parts of your website where you collect data. Review the data handling process and the service providers you use. You and the expert will then evaluate whether any of these need to be changed. Together with the expert, evaluate whether you fall under the GDPR's list of categories which require a DPO and a handling register. Then, move on to the implementation.

One more tip

Looking for simple tools that will allow you to document your data handling activity, manage internal privacy, and safeguard documentation of consent? Try these 2 new solutions Internal Privacy Management e Consent Solution by iubenda.

Useful resources

Your first resource should be the website of the European Privacy Authority, which has made a dedicated page available to companies, freelancers, and small businesses with an entire series of tool and information.

Here you can read the GDPR > GDPR - Privacy Regulation text

Click here for a complilation of different European countries' regulations > The General Data Protection Regulation (GDPR)

Click here for software to help you draw up the DPIA, which is offered by the French government but is available in several languages > DPIA creation software

Finally, the British Information Commissioner's Office has a series of checklists that will help you understand where you stand and what you need to do > Data protection self-assessment

---

We'd say the best way, and maybe the only way, to understand whether or not you fall under the categories laid out by the GDPR's, or more generally, to understand how to comply, is to consult a privacy expert. This post is intended as a summary, so that you can be informed and aware in order to pose clear and targeted questions to the expert you contact.