FFW™

How to Prepare for GDPR

There's been a lot of talk around some new legislation that's coming up in the European Union. The General Data Protection Regulation, or GDPR, is a new law that governs **how the data of European citizens must be handled, regardless of the nationality of the organisation that is handling the data.**

GDPR lays out very specific guidelines for the acquisition, management, and use of data that is either tied to any resident of the EU, or collected by a company that operates in the EU. Noncompliance with this new law can mean large fines.

This whitepaper will help you understand the new law and what it means for the way your organisation collects, stores, and uses data. It will cover some of the legal definitions around GDPR, includes tools for evaluating whether your organisation is GDPR compliant, and suggests next steps for businesses that need to become compliant.

FFW

Contact FFW

To prepare for GDPR, you must understand which data you create, where and how you process and store it, and how your organisation can support users' rights with your systems.

For help complying with the new regulations, contact FFW. We provide services to help organisations of all sizes and kinds prepare their data systems for GDPR.

Learn more at:

ffwagency.com facebook twitter linked in

What is GDPR?

In 2016, the European Union (EU) approved its General Data Protection Regulation (GDPR) to protect European citizens' data.

The law is designed to ensure the **"protection of natural persons with regard to the processing of personal data and on the free movement of such data."**

But what does that mean?

Simply put, GDPR is a new law that protects the data of the people of Europe. There are two types of legislation in EU:

Directives, where member parliaments need to pass legislation

Regulations, which are immediately applicable within the member states

GDPR is a regulation, which means that from the time that it is applicable as law, it's a law in every single member state of the EU. But since the law is focused on the protection of data, it applies to any organisation that collects, stores, or leverages the data of an EU citizen, even if that organisation is based outside the EU.

When reading about GDPR, you may encounter the phrase **"Rules relating to the protection of natural persons with regards to the processing of personal data."** This is an important phrase, as it includes several legal distinctions that organisations need to take into account:

Natural person is a living individual

Personal data is any information relating to an identified or identifiable natural person. This could be their:

- Name
- Identification number
- Location data
- Online identifier
- Or any other factor specific to the identity of that natural person

Processing means any operation or set of operations which is performed on personal data. This includes:

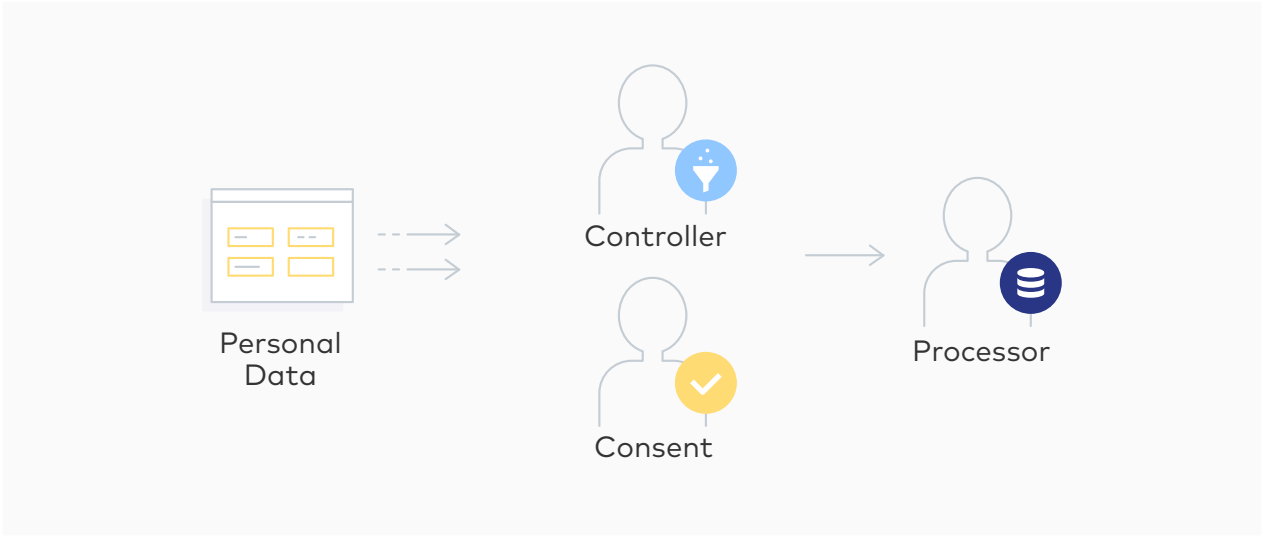
- Collection
- Recording
- Organisation
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission
- Dissemination or otherwise making available
- Erasure or destruction of that data

Understanding the scope "personal data" and "processing" can help organisations gain a better understanding of how massive this law is. **The regulation will go into effect on 25 May, 2018.**

Before that happens, organisations need to make sure that they're fully compliant. For companies that experience breaches that result in the loss of personal data (such as Talk Talk, which lost 170,000 people's data), the fines will be painfully steep. **Low-penalty fines are €10M or 2% of the annual turnover** - whichever is higher. For high-penalty fines, those numbers double.

Who needs to comply with GDPR?

In a word: everyone. If there's even a chance that your organisation has the data of an EU citizen somewhere in your systems, you need to make sure you're compliant. There are a few more important definitions to understand when preparing for GDPR compliance.



Controller

The controller is the organisation or individual that is "in charge" of the data. Officially, a controller determines the purposes and means of the processing of personal data.

A controller can be a natural or legal person, public authority, agency, or other body, which can act alone or jointly with others.

For example, when you downloaded this whitepaper from FFW, you gave us your name, your email, and possibly some information about your employer. That makes us the controller on the data that we collected from you when you filled out the download form on our website.

Consent

The controller is responsible for processing data lawfully, fairly and in a transparent way. Controllers are able to exhibit lawfulness if a data subject has given consent to the processing of his or her personal data. Consent must be freely given and must give a specific, informed and unambiguous indication of the data subject's wishes.

The law here is very clear about what constitutes consent: users must make a statement or perform a clear, affirmative action stating that their data can be used.

The guidelines around consent means that there has to be a clear privacy notice to users when they input their data. The notice must state very clearly why consent is being asked, and what is going to happen with that data. Additionally, people always have to opt-in, rather than opting out. Clever wording and pre-checked boxes would be considered in violation of the consent rules. As a controller, have to be clear that you're asking for permission to use your visitors' data, and what it means if you ask for it.

Processor

The processor is the organisation or person who manipulates, stores, or destroys the data. As with a controller, a processor can be a natural or legal person, public authority, agency or other body.

A processor can actually manipulate information on behalf of a controller.

Another example of this is that some of the services that we offer at FFW include the storage and retrieval of our clients' data on their own customers. That makes us a processor for other parties, even though we aren't performing any processes on the data for our own organisational benefit.

GDPR is about protection and privacy

GDPR is very explicit about the fact that organisations should be able and ready to demonstrate compliance to the requirements of the law. The goal here is to be proactive, not reactive: if someone contacts you to make sure you're compliant with GDPR, you should be able to demonstrate on the spot that your organisation is following the six principles of GDPR.

According to GDPR, all data...

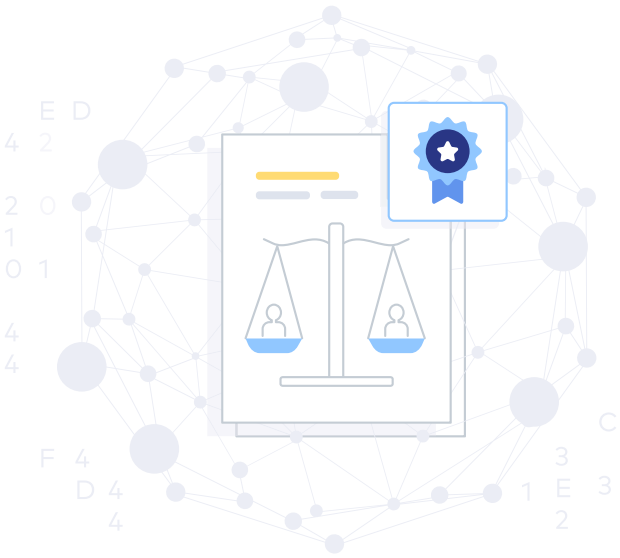
1. Should be processed lawfully, fairly and in a transparent way
2. Should be collected for specified, explicit and legitimate purpose
3. Should be kept up to date
4. Should be limited to what is necessary
5. Should not allow identification of people for longer than necessary
6. Should be processed in a way that ensures appropriate security

When translated, these principles can be boiled down into the following idea:

Data should be collected with explicit consent, and all users should know exactly what their data will be used for. Data collection and retention should be limited only to what your organisation absolutely needs to know about a user. Your organisation should be able to demonstrate that a request for consent was presented clearly, and that that data isn't being sold, modified, or otherwise misused. Systems shouldn't rely on outdated or years-old data for marketing purposes, and if users wish to update their data or withdraw consent, they should be able to easily do so.

And above all, the data needs to be kept in a safe place and processed in a way that safeguards the people to whom the data belongs.

Understanding your users' rights



The GDPR rules were designed around European citizens' rights with regards to their personal data. These are:

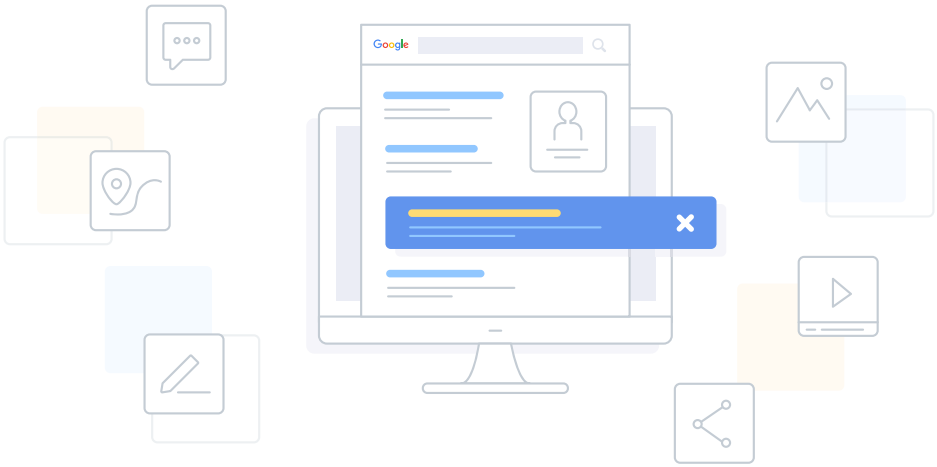
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making, including profiling

In addition to ensuring that your organisation follows the rules around collecting, storing, and manipulating data safely, you also need to make sure you have systems that allow European citizens to exercise their rights with regards to their data. **You'll need to make sure that you have processes, procedures, and training in your team so that users can exercise their rights.**

Additionally, all forms of communication would need to be in a concise and easily accessible form. Use clear and plain language, even on legal documents — you may need to have these revised so they're more accessible to the general public.

An example of building a framework for data rights

For an example of how to make sure your system is compliant, look no further than Google. In May 2015, the EU Court of Justice ruled that search engines are responsible for the content they point to and thus they need to comply with EU privacy laws. Specifically, Google was asked to comply with the right to be forgotten.



According to Reuters, "Internet companies can be made to remove irrelevant or excessive personal information from search engine results... The Court of Justice of the European Union (ECJ) upheld the complaint of a Spanish man who objected to the fact that Google searches on his name threw up links to a 1998 newspaper article about the repossession of his home." Under this ruling, any non-public figure "should be able to remove their digital traces from the Internet."

To comply with users' right to be forgotten, Google created a framework to remove search results from the EU index, and created a process for users to request that their information be taken down.

This is a clear example of how one massive organisation established processes and procedures for people to exercise their rights — and if someone can remove their information from Google, they should be able to remove their information from your systems, too.

Implement an 8-step preparation plan for GDPR

The first step in preparing for the new GDPR is to evaluate your existing policies and procedures. What data do you collect, and why? Is that data secure? Can users scrub their data from your systems? Establish processes, procedures, and conduct staff training so that your organisation is able to deal with people exercising their rights.

Beyond that, there are a few key things you need to do to prepare your organisation:

1. Raise awareness

Make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have, and you need to have their buy-in to make needed changes to your systems.

2. Conduct an information audit

Document what personal data you hold, where it came from and who you share it with. As part of this, you need to review your current privacy notices and put a plan in place to make any necessary changes. Also check what procedures you have in place to ensure that European citizens can exercise their rights on your site. It should be simple for users to provide, update, or delete their personal data from your organisation's systems.

3. Put in a plan for handling access requests

If you get an access request from an individual or from an official organisation that needs to verify compliance, you'll need to have a plan in place. Make sure create or update any procedures you have for supplying data, and plan how you'll handle those requests if or when they come in.

4. Identify lawful basis of processing

Understand how you're processing data, for what reasons, and make sure that your users are providing explicit consent for those actions. Before GDPR goes into effect, you need to make sure that you're processing data lawfully, have documentation in support of that, and ensure that you've updated your privacy notice to explain it.

5. Check your systems for minors

This is a very important step, and one that some organisations may overlook. Depending on how you collect data, you may need to put systems in place to verify individual's ages and obtain parental or guardian consent for children whose data you may collect.

6. Develop a plan for data breaches

No organisation wants to have their data compromised. Nevertheless, you need to make sure first that your data is as protected as possible, and secondly that you have procedures and systems to detect, report and investigate a personal data breach. To ensure that your systems are compliant with the protection rules, familiarise yourself with the latest guidance from Article 29 Working Group. Additionally, map out how you'll implement Privacy Impact Assessments for your organisation.

7. Data protection officers

Designate someone (within your organisation or some legal entity) to take responsibility for data protection compliance. Assess where the role will sit within the organisational structure, and document who your DPO is.

8. Understand international guidelines

If your organisation operates in more than one Member State, determine your lead data protection supervisory authority. Not sure where to start? In December 2016, the Article 29 Working Party ("WP29") published its Guidelines for Identifying a Lead Supervisory Authority to help organisations with this determination. To make the process of identifying a supervisory authority easier, you need to understand where your organisation makes decisions regarding processing activities.

Appoint a representative

Organisations that aren't established in EU but that operate in EU, or that process data of people who are in the EU, must find a representative within the EU.

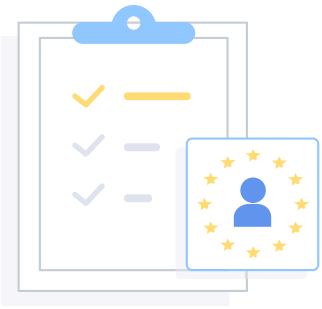
According to GDPR article 4:
"Any natural or legal person who resides in one of the Member States can be appointed as a representative in the Union for a non-EU-based company."

It's the representative's responsibility to provide any requested information that may be requested by a supervisory authority.

Once a representative has been identified, you need to designate that person as your organisation's representative in writing. A representative represents the controller or processor with regard to their respective obligations under GDPR.

A few notes about representatives:

- A representative must be established in one of the EU Member States where your data subjects are located
- It's your responsibility to appoint a representative who is without prejudice towards any legal actions that could be initiated against your company
- A representative will be subject to any enforcement proceedings in the event of non-compliance by the company
    - This means both your company and your representative could be subject to penalties if you don't abide by the law



As GDPR comes closer, there are plenty of services appearing in the EU for organisations that need to designate representatives.

Next steps

To prepare for GDPR, you must understand which data you create, where and how you process and store it, and how your organisation can support users' rights with your systems.

We recommend beginning by identifying how personal data flows through your website.

Once you identify what data you're using and how, you can begin to create systems to better protect your users' privacy, and build processes for users to access, update, or remove their data from your systems.

If you need help with any step of complying with the new regulations, contact FFW. We have teams ready to help you evaluate your current data collections practises and ensure you abide by the law.

To get started, contact us. One of our GDPR experts will be in touch to help you figure out how to move forward.