Bean Counters
Accounting for your Success

What is GDPR?

The GDPR comes into force in May 2018. It's a wide-ranging regulation designed to protect the privacy of individuals in the European Union (EU) and give them control over how their personal data is processed, including how it's collected, stored and used. It affects every company in the world that processes personal data about people in the EU.

What does GDPR mean?

Although GDPR might seem scary at first, many see it as a positive step forward for data protection. Some of the key areas GDPR covers are:

- **personal data about EU-based people (absolutely all of it)**
  This includes your customers, employees, suppliers and any other individual you collect personal data from. Personal data includes names, contacts, medical information, credit card or bank account details and more.
- **how you collect personal data**
  You can only collect personal data if you have a legal reason to do so. You might need it for a sales contract, for example. Or your customer may have asked you to send them some information on your product or service. In all cases, you must make it clear what the personal data will be used for – and only use it for that purpose.
- **user contracts and terms and conditions (on websites, for example)**
  These need to be simple, clear and easy to understand – with no complicated legal text.
- **the right to know**
  Individuals can ask a business what information is being held about them. This isn't a new right, but organisations must now respond within one month and can't charge a fee (which they used to be able to do).
- **the right to erasure**
  Customers can ask a company to delete all stored personal data about them, unless the company needs to keep that information for legal reasons, such as tax.
- **data portability**
  Individuals can request a digital copy of their personal data to use however they like, including transitioning to a new service provider.
- **data breach**
  You're obliged to report certain types of data breach to the relevant supervisory authority.

The UK government will be replicating GDPR into UK law prior to Brexit, so if you're a UK company, Brexit won't impact your obligation to comply.

GDPR and data protection

It's important to understand the spirit of GDPR. The legislation came into existence because of the way personal data has been treated in the past. Many companies treated personal data as a resource they could utilise without regard to the rights of individuals.

For example, some companies sold customers' email addresses, allowed sensitive data to be seen by unauthorised people, and failed to adequately protect data against hackers.

GDPR gives control of personal data back to the people who own it and requires organisations to make data protection a core part of their operations and processes. This is likely to affect big, data-driven organisations first. But small businesses aren't exempt. We've set out some steps below that you can take to make sure you're prepared.

Goes GDPR affect data security?

Data security is a big part of GDPR. If you process personal data of people in the EU you have a duty to keep it safe so it's important to ensure that any personal data held by you is securely stored.

GDPR also governs *where* companies store personal data, and what safeguards you must have in place in order to store and process that personal data outside of the EU. For example, if you're transferring personal data to a US-based company (that will store and process it in the US), you should check that they're certified with Privacy Shield, which is a mechanism designed to allow data transfers from the EU to the US.

Summary of GDPR for small business

There are many aspects to GDPR, but it really boils down to being clear and ethical with the personal data you process – that means treating it as you'd treat something valuable of your own. Some initial practical steps you can take to get GDPR compliant are:

Check products and services

- Check which of your products or services collect and process personal data.
- Ensure you have a legal basis for the processing of personal data.
- Ensure you can comply with the obligations to your customers as set out in the GDPR (such as the right of access and the right of erasure).

Review notices and contracts

- Update your internal and external notices for GDPR compliance.
- Ensure your customer contracts are GDPR compliant.

Assign responsibility

- Make someone in your organisation responsible for data protection and privacy.
- Consider whether you need to appoint a Data Protection Officer – check out the ICO's guidance for more info.
- Provide data protection training for staff.

Take care over security

Ensure systems that collect, process and store personal data are secure.

GDPR resources for small businesses and advisors

You can get useful information on GDPR from:

- The UK Information Commissioner's Office (ICO) – 12 steps to prepare for GDPR.
- The Federation of Small Business (FSB) – How to prepare for GDPR.

You should also talk to your legal advisers to ensure you are compliant before May 2018.