What does GDPR mean for your business?

Preparing for General Data Protection Regulation

The EU's unified framework of personal-data protection comes into effect 25th May 2018.

What is GDPR?

The General Data Protection Regulation (GDPR) has been introduced by the European Union (EU) to provide a unified framework of personal data protection. The regulation is expected to have far-reaching consequences for businesses, charities and individuals.

It comes into effect in 25 May 2018 – and as at October 2017, a large proportion of UK businesses aren't fully prepared. According to Experian, 48% of businesses are 'somewhat ready', while over 25% are 'not very' or 'not at all'[1].

How does GDPR protect individuals?

GDPR strengthens an individual's rights over their personal data, including

- The right to be informed about what data a business has collected about them
- The right to access this data
- The right to rectification – to change any inaccurate data
- The right to erasure – to have data deleted
- The right to restrict processing – to stop a business processing their personal data
- The right to data portability – to be able to move data to another organisation
- The right to object to their data being collected or used
- Rights in relation to automated decision making and profiling
- The right to remedy – to be compensated for any unauthorised collection or use of data

Personal data relates to an identified or identifiable individual, rather than data referring to a company. Names and addresses can be considered personal data. Also, data that refer to a person, e.g. ID numbers and attributes such as gender, economic and social status are also considered personal data.

Is GDPR applicable to a business or charity?

GDPR covers all information recorded electronically, and most recorded physically,(which refers to any written information including the sales persons famous “little black book”) that can relate to or identify any individual from the EU. This means that any business or charity wishing to interact with anyone from the EU must comply, even if based elsewhere. UK businesses and charities have to adhere, regardless of the ongoing negotiations around Brexit.

What happens if my business isn’t compliant?

The ‘right to remedy’ means that individuals have the right to ask for compensation. There’ll also be significant fines of up to 4% of revenue or €20m for any organisations found to be non-compliant.

As well as a potential fine, failure to comply with GDPR also runs the risk of damaging your business’ reputation, as well as relationships with suppliers and partners. Getting on top of this regulation and ensuring your business is compliant before May 2018 should be a priority.

When will GDPR apply?

GDPR comes into effect in May 2018. Businesses across the country are gearing up to achieve compliance ahead of the effective date.

What can I do to prepare my business?

There are steps you can start to take to make sure you’re not caught out. A good starting point is to make checklists of the personal data you hold, its source, and how you use it. You can then review your existing processes and develop new processes, if needed, to comply with the regulation. Put simply, you must comply with the regulation when you’re using any personal data within your business.

Work out what data you hold on your customers
Most businesses across the UK, regardless of size or nature, will hold data on their customers. This could be as simple as email addresses and phone numbers, or more sophisticated data storage such as tracking customers’ online habits when visiting your website, or saved card details.

Lawful Processing of personal data
You should consider the reasons why you are capturing and processing personal data. Note that there are multiple legal bases for processing data which you may be able to rely upon. If you need to rely on consent to process personal data (perhaps for some forms of marketing), you need to ensure that consent is freely given before the data is processed, unambiguous and can be withdrawn at any time.

Allowing customers access to their data
If a customer wants to access the data you hold for them, you must have a process to provide access within one calendar month. If they wish to withdraw their consent and delete the data you should be able to satisfy those requests.

Employee data
The regulation also includes your employee data, which you need consent to acquire and protect. These aren't the only actions you have to take, however.

The Information Commissioner's Office (ICO) has put together a plan of 12 key actions you can start right away:

1. **Awareness** – make sure that decision makers and key people in your organisation are aware that the law is changing. They need to appreciate the likely impact.
2. **Information you hold** – document what personal data you have, where it came from and with whom you share it. This may need an information audit.
3. **Communicating privacy information** – review your current privacy notices and plan any necessary changes.
4. **Individuals' rights** – check your procedures to make sure they cover all the rights individuals will have under GDPR, including how you'd delete their data if requested, or provide data electronically and in a commonly used format.
5. **Subject access requests** – update your procedures, as well as planning how you'll handle requests within the new timescales and provide any additional information.
6. **Lawful basis for processing personal data** – identify the lawful reason as to why you're processing personal data, document it and update your privacy notice to explain it.
7. **Consent** – review how you seek, record and manage consent, and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. **Children** – do you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data-processing activity?
9. **Data breaches** – make sure you have the right procedures in place to detect, report and investigate a personal data breach. Make sure you've shared these processes with the appropriate members of your team.
10. **Data Protection by Design and Data Protection Impact Assessments** – familiarise yourself with the ICO's code of practice on Privacy Impact Assessments, as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.
11. **Data-protection officers** – designate someone to take responsibility for data protection compliance in your business. Larger organisations might need to appoint a

formal data-protection officer – visit the EU Commission website to see if your business will need to do this.

12. **International** – if your business operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

All businesses are subject to the same principles, and the steps and sources of information here are by no means exhaustive and shouldn't replace professional advice. For more help, we recommend speaking to a professional adviser or your accountant.

What happens to previous data regulation?

GDPR replaces the 1998 Data Protection Act.