mercia
Wilmington Professional

What does GDPR mean for businesses

New data protection rules from General Data Protection Regulation (GDPR) will replace the Data Protection Act (DPA) in the UK. It is designed to safeguard personal data of citizens from EU member states, with particular emphasis on transparency and accountability. It applies to all businesses in the EU and non-compliance will lead to substantial fines.

What is GDPR?

The new GDPR is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The regulation was adopted on 27 April 2016 and will become a law without exception in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. Digital minister Matt Hancock has also confirmed that the UK will replace 1988 Data Protection Act (DPA) with legislation that mirrors GDPR, post-Brexit. It will effect all businesses in the UK and ensure they seriously consider data protection.

This means that any business, big or small, will be required to comply with GDPR - which deals with secure collection, storage and usage of clients' personal data.

Failure to comply with the regulation can result in heavy fines of up to €20 million or 4% of the businesses' annual turnover (whichever is higher amount).

Some of the key requirements of GDPR are:

- Businesses with over 250 employees must assign a Data Protection Officer (DPO) who will be responsible for ensuring that the business is collecting and storing personal data responsibly.
- Any data breaches must be immediately reported to the Information Commissioner's Office (ICO) within at least 72 hours.
- Clients reserve the 'right to be forgotten' and may withdraw their consent of use of their personal data at any time.
- The time businesses have to respond to a Subject Access Request (SAR) is now reduced to 30 days.

GDPR builds around existing data protection principles from DPA. The key data protection principles under **Article 5 of GDPR** are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

What is included in 'personal data'?

Any personal data falling under the scope of DPA will also apply to GDPR. This includes client data such as name and contact details, as well as HR records of employees that your business holds.

Unlike DPA, GDPR's definition of personal data is now more detailed, making consideration for advances in technology and the way businesses collect information from clients online.

For example, personal data now also includes information such as online identifiers from your website, such as a visitor's IP address or cookies that collect user information when they visit your website.

How does it affect your business?

GDPR maintains that the Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations.

Essentially GDPR applies to all businesses in the UK that hold or process personal data within the EU. According to GDPR, 'controllers' decide how and why client data is processed, while 'processors' act on behalf of a controller.

The following table differentiates the roles and levels of responsibility for GDPR between processors and controllers:

Processors	Controllers
Maintain records of personal data and data processing activity	Ensure that contracts with processors comply with GDPR
More legal liability in case of a data breach	

Whether your business is a 'controller' or a 'processor' of personal data, GDPR has specific rules for each and you must ensure that your business is aware of your responsibility and meet the terms of GDPR that apply to your business.

If you are unsure whether GDPR applies to you, consider how regularly you deal with personal data, including present and past employees and partners, not just client data.

Exemptions

GDPR will not apply to personal data under contractual obligation such as transactional communications. For example, you don't need specific consent from clients for sending them their invoice.

GDPR **requires obligations** to provide comprehensive, clear and transparent privacy policies and detailed records of processing activities. If your organisation has more than 250 employees, you must maintain internal records of your processing activities. However for businesses with fewer than 250 employees the records of processing activities are not required unless they relates to 'higher risk processing' such as:

- processing personal data that could result in a risk to the rights and freedoms of individual; or
- processing of special categories of data or criminal convictions and offences.

Preparing for GDPR

While the legislation won't kick in until May next year, businesses are advised to plan ahead and ensure that they have taken adequate measures to ensure compliance with GDPR. To prepare your business for GDPR, there are a number of steps to be taken so that the personal data you hold is acquiescent with new legislation. Some of the actions that your business must take include:

Create awareness

Make sure that stakeholders and key decision makers within your business are aware of the changes from DPA to GDPR.

Businesses are also advised to look at areas that are likely to be impacted by GDPR and identify potential compliance issues. Any compliance issues must be dealt with before May 25 2018.

Review how you process data

You will need to review the personal data you hold, where it came from and who it is shared with. GDPR also requires businesses to document records of all data processing activities. This will help businesses to comply with GDPR's data protection principle on accountability, which requires businesses to show how they comply with the data protection principles of GDPR. For example, having effective policies and processes in place for data documentation and retention.

Ensure that you have consent from clients

You must review how your business seeks, collects and manages consent. If existing consents are not meeting GDPR guidelines, you will need to refresh existing consents from your clients based on GDPR guidelines. You must also have documented proof of the fresh consent. GDPR clarifies the scope of consent – it must be freely given, specific, informed and unambiguous.

For example, you can contact clients by phone, email or post and seek fresh permissions that meets GDPR standard. ICO have published **detailed guidance on consent** on GDPR including a consent checklist that you can use to review your practices.

Clients also should also be fully aware of what they're signing up for. Post-GDPR, you must include an Information Notice which clarifies to clients their rights under GDPR when they register their details with your business. We have included a **checklist** which looks at what details you need to include in an Information Notice to make sure you are compliant with GDPR requirements. The checklist has been made available as a Word document so it can be edited and personalised for your business should you want to share it with your clients.

Communicate privacy information clearly

You must review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. Currently, when businesses collect personal data, they are required to give clients information on your identity and how you intend to use the information using a privacy notice. Under GDPR, businesses will need to update the privacy notice with additional information including lawful basis for processing the data, data retention period and that clients have the right to complain to the ICO if they think there is a problem with the way their data is being handled. GDPR requires this information to be provided in concise, easy to understand language in the privacy notice.

Read the ICO's **Privacy notices code of practice** that provides more information on the new requirements.

Further guidance

While this document briefly summarises GDPR requirements for businesses, we recommend visiting ICO's dedicated website on GDPR – **Data protection reform** – where you can find detailed, up-to-date information on preparing your business for GDPR. The website also offers a free **self-assessment tool** for evaluating whether your business is ready and prepared for GDPR.