A Guide to the General Data Protection Regulation for Businesses

This guidance note explains what is meant by personal data and what the GDPR will entail for businesses. It includes a checklist on what businesses should do before May 2018.

The General Data Protection Regulation (the GDPR) will come into force in the UK in May 2018. The way you, as a business, collect, store and use your data will be subject to additional scrutiny. All businesses should now treat data compliance as a commercial necessity: non-compliance could mean a substantial fine, whatever the size of your business.

One of the aims of the GDPR is to consolidate data protection laws in the various European Union (EU) territories all of which implemented the previous EU data protection directive differently.

This guidance note explains what is meant by personal data and what the GDPR will entail for businesses.

What is Personal Data?

"Personal data" includes:

- a wide range of information that is collected by organisations located in the EU (regardless of whether the data is used in the EU); and
- the personal data of people located in the EU (regardless of the location of the organisation collecting it).

Most businesses collect personal data about their customers in some form or other. Examples include:

- all information that can be used to identify a person (either by itself or when combined with other information already held);
- email addresses;
- IP addresses;
- genetic information and other data (such as biometric data), which are treated as 'special categories' of personal information;
- health records; and
- cultural, social and economic information.

This information might be stored in emails, excel spreadsheets, software, invoices, delivery notes, contracts etc. It could be in the keeping of an organisation's management team, HR team or staff. It could be in the client contacts lists or in employees' personal contacts/address lists. Such customer databases might include email addresses, home addresses and telephone numbers as well as details of the customer's purchase history and order details.

PEARSON
SOLICITORS AND FINANCIAL ADVISERS

What Are the Current Data Protection Laws?

The Data Protection Act 1998 (the 1998 Act) sets out how businesses and the government can use personal information. It provides a series of data protection principles to ensure that such information is used fairly and lawfully, accurately, safely and securely, for limited, specifically stated purposes and in ways that are adequate, relevant and not excessive.

The 1998 Act also ensures that data is not kept for longer than it is needed and is handled according to people's data protection rights.

Sensitive information, for example relating to health or religious beliefs, must be treated even more carefully.

The 1998 Act also gives individuals rights to find out what information is held about them (subject to certain exceptions).

The New General Data Protection Regulation

The GDPR is a new European Union (EU) law that regulates how businesses collect, store and use information within the EU and globally. It will force businesses to get to know their customers better by understanding what they want. Businesses must gain and maintain their customers' trust by protecting the personal information they hold.

The principles to be followed under the GDPR are broadly similar to those under the 1998 Act. However, there will be a new principle of accountability meaning that organisations have to be able to demonstrate compliance with the GDPR through evidence.

The GDPR will have direct effect in the UK from 25 May 2018.

The Data Protection Bill 2017

The UK government has also published a new Data Protection Bill 2017(***3**) (the Bill) (which was published in draft on 14 September 2017). As part of the Bill, which will replace the 1998 Act, the government will update data protection law and apply the GDPR standards.

When announcing the Bill, Matt Hancock, Minister of State for Digital summed up its aims as follows:

"Our measures are designed to support businesses in their use of data, and give consumers the confidence that their data is protected and those who misuse it will be held to account.

The new Data Protection Bill will give us one of the most robust, yet dynamic, set of data laws in the world. The Bill will give people more control over their data, require more consent for its use, and prepare Britain for Brexit. We have some of the best data science in the world and this new law will help it to thrive."

The government explained what the Bill will do as follows (***1**):

- make it simpler for individuals to withdraw consent for the use of personal data;
- allow people to ask for their personal data held by companies to be erased;
- enable parents and guardians to give consent for their child's data to be used;
- require 'explicit' consent to be necessary for processing sensitive personal data (Note: there will be no reliance on customers having given 'implied' agreement for their personal data to be retained and used. Their consent must be given freely and be "specific, informed and unambiguous");
- expand the definition of 'personal data' to include IP addresses, internet cookies and DNA;

- update and strengthen data protection law to reflect the changing nature and scope of the digital economy; and

- make it easier and free for individuals to require an organisation to disclose the personal data it holds on them;

- make it easier for customers to move data between service providers.

The Bill is progressing through Parliament (*2).

What Do the GDPR Mean for Businesses?

All businesses, SMEs and PLCs alike, will be subject to the GDPR. Smaller businesses might not have as much money to invest in cyber security and training – but they will be subject to the same fines under the GDPR. All businesses must prepare for the regulations coming into force – and should do so well in advance of May 2018.

The biggest issue is the increase in accountability for organisations in how they handle personal data. When using a person's personal data, businesses will have to:

- understand what risks they might create for that individual by using that data; and

- take steps to minimise those risks.

The practical requirements and effects of the GDPR (effective from May 2018):

- Regulators will be able to force businesses to demonstrate that they are complying with the GDPR. They will be able to fine those who cannot show compliance or who are in breach of the regulations.

- Whilst notification or registration will no longer be required under the GDPR, businesses will be required to maintain detailed records about their data processing activities and may have to appoint a specific data protection officer.

- Organisations will have to establish and document the lawful basis for processing personal data.

- Individuals will have increased rights under the GDPR and businesses will have to be ready to deal with them.

- Any cross-border data transfer activities will also have to be documented.

- Certain types of data breaches will have to be reported by businesses to the data protection regulator and, in some cases, to the individuals involved.

- When businesses agree to process data on behalf of someone else, or ask a third party to process data on their behalf, the agreement covering those arrangements will have to be legally binding and include specific obligations concerning data privacy and security.

- The GDPR talks about 'privacy by design'. This means businesses must ensure they consider the protection of personal data at the inception of new products and processes - not as an afterthought. Data privacy must be embedded into the culture and operations of the organisation. This in turn will mean businesses must monitor the effectiveness of the measures they introduce and provide training for staff.

- In certain instances, where large scale processing or processing of sensitive data is required, organisations may have to undertake data protection impact assessments.

The Risks of Non-Compliance With the GDPR

The incidences of cybercrime are increasing. If criminals manage to "hack" into business systems and steal personal data, the customers of the business could also be at risk of cybercrime. For example, the thieves could use the stolen personal data to access customers' bank accounts.

The GDPR increase the powers of the regulators to impose penalties on those who compromise personal data in breach of the GDPR. For lesser offences, those in breach could be fined up to €10 million (£7.9 million) or 2% of their global turnover (whichever is greater); for significant offences, the fine will be up to €20 million or 4% of their turnover (whichever is greater).

Financial penalties might not be the only consequence: the commercial reputation and standing of the business could be affected.

Checklist: What does your business need to do before May 2018?

To ensure compliance with the GDPR, businesses should start to prepare for the GDPR *immediately* (*4)

- Read the GDPR and ensure you understand what is required.
- Consider appointing one of your management team to oversee compliance (in some cases this will be mandatory) – but if you do, ensure that he or she is reporting to the board or business owners regularly.
- Keep up to date with the progress of the Data Protection Bill through Parliament.
- Audit your data. This is an onerous exercise: do not underestimate it. You will need to be able to identify "personal data" then find out what data you store.
- Review how you collect information. Is it by website cookies? By email? Through your contracts?
- Review how you manage your data storage (and where it is stored).
- Document these processes.
- Check whether you are allowed to keep the data. You might have to justify why you have it and whether you have customer permission to keep it.
- Review your privacy policies and notices. Do they need to be changed?
- Train your employees on the data protection laws and ensure they understand why data protection is so important for you and your customers.
- Review your systems' security arrangements. Are they safe from hackers?
- Train your employees on the risks of cybercrime and how to avoid it. Give refresher courses on a regular basis.
- If a customer asks you to delete or remove their personal data from your records – do so immediately. Set up a system for doing this. Ensure someone within your business has responsibility for this task.
- Review data regularly. If you don't need it, delete it.

- The GDPR will affect how you handle your digital marketing. Work closely with your marketing team to ensure compliance.

- Have you prepared for a cyber attack? (All cyber attacks must be reported to the Information Commissioner's Office (ICO)).

How Does the Impending Brexit Affect the GDPR?

The UK is subject to EU laws and required to enforce the GDPR by virtue of its membership of the EU.

When the UK leaves the EU, under the provisions of the draft EU (Withdrawal) Bill, all EU laws are expected to be fixed in UK law as at the date of the official 'Brexit' from the EU. (On current information, this date will be at the end of March 2019).

The draft wording of the EU (Withdrawal) Bill gives broad powers to the government to make changes to the EU law. While there is significant opposition to this wording, we cannot yet say whether changes will be made to the GDPR after Brexit.

In any event, any organisation in the UK that processes information about EU citizens will have to abide by the GDPR - even after the UK has left the EU.

The Role of the ICO

The ICO is the UK's independent body that was set up to uphold information rights. It is responsible for investigating concerns about data usage and for taking enforcement action.

The ICO is undertaking a consultation on GDPR guidance on contracts and liabilities between controllers and processors, which closes on 10 October 2017. You can access the consultation using this link:

https://ico.org.uk/about-the-ico/consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/

How Can We Help You?

The list of action we have set out above can seem – and is – a daunting exercise. The good news is that there is still plenty of time to take action.

Our commercial team at Pearson Legal can guide you on how best to prepare your business for the introduction of the GDPR. For example, we can:

- undertake an information audit to determine what your additional obligations under the GDPR will be;

- help you to document what personal information you use and how you use it;

- analyse your procedures for obtaining consent and update them, where necessary;

- review your privacy notices and advise of changes necessary to comply with the GDPR;

- review the data protection obligations in your contracts and make sure you are protected when the GDPR comes in - both as a data controller and a data processor;

- help you draft or update policies and procedures including ones to deal with new individuals' rights like the 'right to be forgotten';
- advise you on what to do in the event of a data breach;
- identify your requirements for appointing data protection officers;
- help you to identify your organisation's lawful basis for processing personal data, document it and update your policies to comply with it.

Contact

For more information about data protection and how best to prepare for the new regulations, contact:

Keith Kennedy on 0161 785 3500 or keith.kennedy@pearsonlegal.co.uk

Sources/References

***1** https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

***2** https://services.parliament.uk/bills/2017-19/dataprotection.html

***3** The text of the Data Protection Bill: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_1.htm

***4** You can discuss these steps with one of our team. The ICO have published more information on action to take on their website.

PEARSON
SOLICITORS AND FINANCIAL ADVISERS