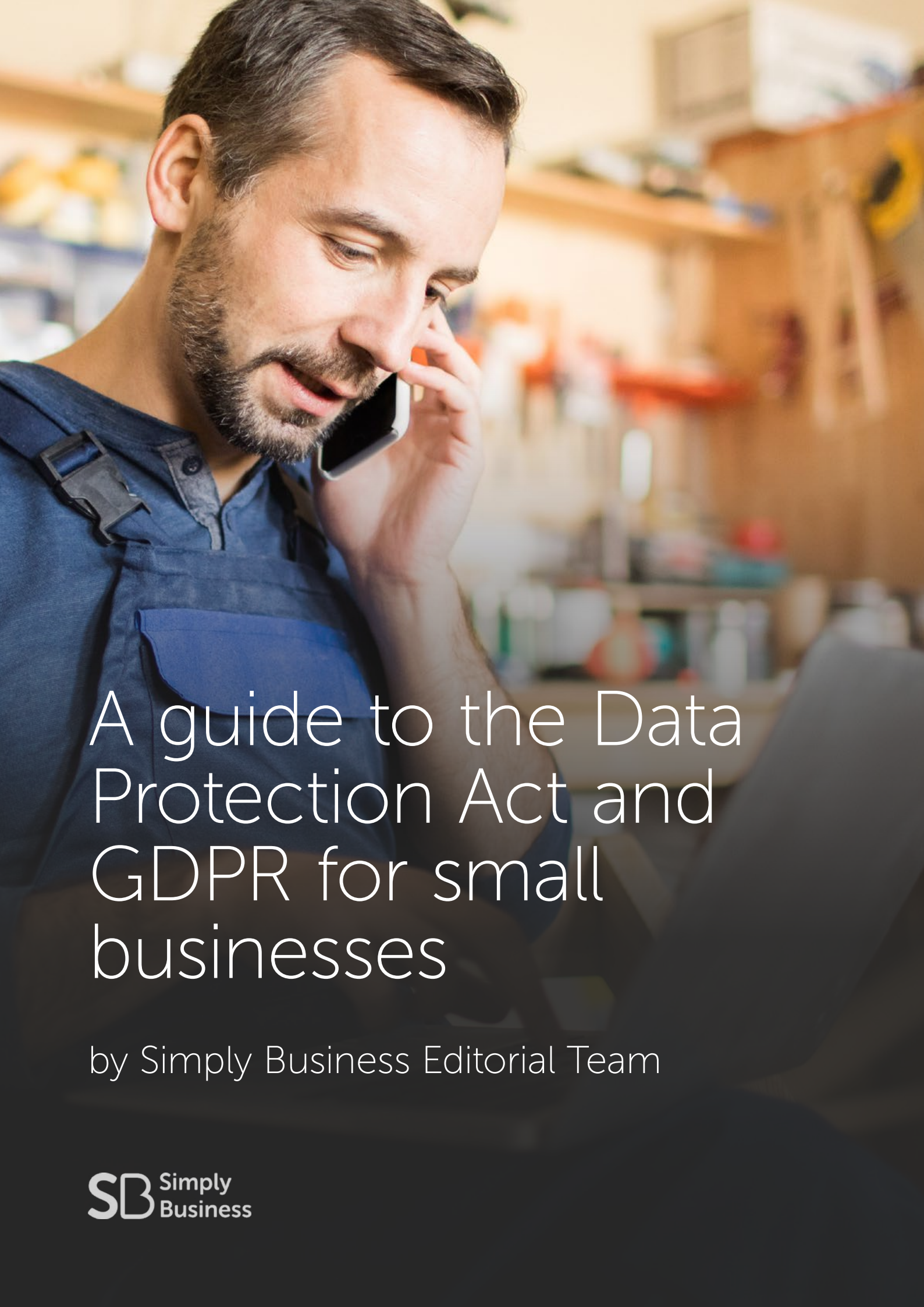

A guide to the Data Protection Act and GDPR for small businesses

by Simply Business Editorial Team

Simply Business

About Simply Business

We're one of the UK's largest business insurance providers. Since we started life in 2005, we've helped three million small businesses and self-employed people find the protection that's right for them, from builders to bakers and personal trainers (we cover landlords, too).

How does it work?

Answer a few questions about your business and we'll show you quotes from a range of insurers. After you buy, our Northampton-based team will be with you through every step of your cover, whether you have questions about your policy or you need to make a claim.

Get a quote

Data protection

If you're running a business, chances are you're also dealing with personal information. Whether that's details about customers, suppliers, or your own staff, it's important to follow certain data protection regulations.

Read on to understand more about the Data Protection Act (DPA), UK GDPR and the key principles you need to be aware of as a small business.

Contents

What is the Data Protection Act 2018?

The Data Protection Act 2018 is a piece of UK legislation that's designed to protect the privacy of personal data. It replaces the Data Protection Act 1998 and now incorporates GDPR legislation into UK law.

In essence, the law aims to:

1. **Give citizens and residents more control of their personal data** – everyone has a right to find out what information the government and organisations hold about them.
2. **Simplify regulations for all businesses to help them protect personal data** – making sure that information is used lawfully, fairly, and transparently.

Although you may think that this only applies to larger companies, in fact most businesses hold some personal data – for example customer contact details, or HR information about staff.

If you do use or store personal information, and this information relates to someone that can be identified, you're referred to in the Act as a 'data controller'.

What does GDPR stand for – and does GDPR still apply?

The European General Data Protection Regulation (GDPR) came into force in the UK in May 2018. However, since the UK left the European Union and the transition period ended on 31 December 2020, the GDPR has now been incorporated into the Data Protection Act 2018.

You may need to comply with both the UK GDPR and the EU GDPR if your business operates in Europe, or you offer goods or services to people in Europe.

What does the Data Protection Act mean for my business?

The Data Protection Act 2018 and UK GDPR applies to any business established in the UK.

The main question to ask yourself is, **how often does your business deal with personal data**? This includes your customer data of course, but have you factored in supplier data? Past and present employees?

If you're collecting any of this data routinely, you need to comply with the UK GDPR, whether the data is stored on a spreadsheet, your computer, mobile phone, or in the cloud. It applies for both manual data collection and automated digital capture.

Even as a small business you must follow the law and take responsibility for handling personal data. Beyond that, it can help you demonstrate to potential and existing customers that you're doing everything you can to protect their data from being lost, stolen, damaged, misused, or shared – this level of trust is invaluable and could even help you bring in more business.

Is your data ‘sensitive’?

The Data Protection Act 2018 offers stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics
- health
- sex life or orientation

Generally, you’ll need explicit consent from individuals if you want to collect or process sensitive information.

The Data Protection Act – employers' responsibilities

As an employer, you'll have a number of unique responsibilities. Firstly, workers have a legal right to access information that their employer may hold on them.

Meanwhile, employers should also make sure that staff comply with data protection regulations in their day-to-day work, and have a duty to monitor the likes of telephone calls, emails, and CCTV where necessary.

Data controllers have a series of important responsibilities, and must follow the seven data protection principles.

The Data Protection Act – 7 key principles

If your organisation deals with personal data, you must consistently act in accordance with the seven key principles set out in the DPA.

1. Personal data must be processed lawfully, fairly, and in a transparent manner

This is among the most important requirements of the DPA. To comply, you must provide people with the name of your business, and details of how their information will be used. You should make it clear that the individual can access and correct the information that you hold about them.

Crucially, you must also tell them if the information will be used in any way that's not immediately obvious. For example, you must tell the individual if their details will be passed on to credit reference agencies.

2. Personal data must be processed for specified, explicit, and legitimate purposes

You must be clear why you're collecting someone's personal data and how you intend to use it. This clearly links to the lawfulness, fairness, and transparency principle mentioned above.

You can't use the data collected for another, 'incompatible', or unlawful purpose. For example, if your purpose changes over time and this isn't 'compatible' with the original purpose, you'll need to get the individual's specific consent for the new purpose.

3. Personal data must be adequate, relevant, and not excessive

You should only collect the bare minimum; you may not collect information that isn't immediately relevant to the specified purpose, and you may not collect more information than you need.

4. Personal data must be accurate and up to date

Any information you hold must be factually accurate, and updated where necessary. Depending on the nature of your business, you may need to develop mechanisms that allow people to update their details quickly.

5. Personal data shouldn't be kept any longer than is necessary

This storage limitation principle states that you shouldn't keep data any longer than needed. If you collected data for a purpose that's time-limited then you should make sure that the information isn't retained beyond that point. Reducing how long you hold data also helps you to reduce the risk of storing personal data that's inaccurate or out of date.

It's good practice to tell people how long you intend to keep the data for and you might find it useful to set retention periods for your data.

6. Personal data must be processed securely

You must take adequate steps to maintain the integrity and confidentiality of personal data. Having an information security policy in place can help demonstrate that you're looking after personal data and reducing the risk of it being compromised.

7. The controller is responsible for GDPR and must demonstrate compliance

This final principle sets out the law when it comes to accountability. As a data controller, you're responsible for what you do with personal data and must demonstrate how you're looking after people's privacy.

More information on the GDPR principles can be found on the ICO website.

How do I get consent from my customers to use their data?

Here are some key things to think about when it comes to collecting individual's data:

- check your consent practices and existing records – and refresh where necessary
- offer people genuine choice and control
- where using an opt-in, don't rely on pre-ticked boxes or default options
- explicit consent means a very clear, specific statement of consent
- keep your consent requests separate from other terms and conditions
- be specific, granular, clear, and concise
- name any third parties who will rely on the consent
- make it easy for people to withdraw consent (and tell them how)
- keep evidence of the consent (who, when, how, and what you've told people)
- avoid making consent a precondition of your business services

Ultimately, consent should put individuals in control, build trust and engagement, and enhance your reputation.

Do I need to register with the ICO?

As well as following the key principles above, you may also need to pay a data protection fee to the Information Commissioner's Office (ICO). The DPA works on the basis that all data controllers notify the ICO, but there are some exemptions. If you're not exempt but you fail to notify the ICO, you risk prosecution.

You may be exempt if you only process personal data for one (or more) of the following purposes:

- staff administration
- payroll
- advertising, marketing and PR
- not-for-profit purposes
- personal, family, or household affairs
- maintaining a public register
- judicial functions
- or if no automated system, like a computer, is used in the processing of data

Registration and the data protection fee

You can use the ICO's online checker tool to see if your business is exempt from registration. Even if you're exempt from paying a fee, you still need to comply with other data protection obligations.

If you do need to register, you'll need to pay a data protection fee. Registration generally costs between £40 and £60 a year.

If you don't comply with the Data Protection Act, you could face serious penalties. The maximum fine under UK GDPR and the DPA is now £17.5 million or four per cent of the total annual worldwide turnover in the preceding financial year, whichever is higher.

GDPR checklist – tips for small businesses

1. Know your data

Demonstrate an understanding of the types of personal data you're holding (such as name, address, email, bank details, photos, IP addresses) and sensitive data (for example health details or religious views), as well as where the data is coming from, where it's going and how it'll be used.

2. Identify when you're relying on consent

If you're relying on personal consent to process personal data (for example, as part of your marketing) then you need to be clear, specific, and explicit as to your purpose.

3. Review your security measures

Make sure you have strong security measures and policies. Broad use of encryption, for example, could be a good way to reduce the risk of a security breach.

4. Meet access requests

Everyone has a right to access any personal data you may hold. The right of access under GDPR states that you must respond to a request within one month. This can only be extended in mitigating circumstances.

5. Train your employees

Staff should report a serious personal data breach within 72 hours. Make sure that everyone knows the process for reporting and who to report a breach to.

6. Conduct due diligence on your supply chain

Make sure your suppliers and contractors are compliant with UK GDPR to avoid being impacted by any breaches.

7. Regularly review your privacy policies

People have a right to be informed of how you're using their personal data. This should be included in your privacy policies and information should be reviewed regularly to make sure it's up to date.

8. Check if you need to employ a Data Protection Officer

Most small businesses will be exempt. However, if your company's core activities involve 'regular or systematic' monitoring of data subjects on a large scale, or which involve processing large volumes of sensitive data, you must employ a Data protection Officer.

For more information, check out these resources from the ICO:

- small business web hub
- data protection checklist
- Privacy and Electronic Communications Regulations

If you're not sure about anything, seek guidance from the Information Commissioner's Office (ICO), or from an independent legal professional.

Related articles

Do you know about these four legal obligations of a business?

Have you got an HMRC scam email, call or text? Here's how to check it's genuine

Consumer Protection Act: summary guide for small businesses

Do I need professional indemnity insurance?

Join our small business community

Article last updated: May 2021

Image credits
Front cover: Seventyfour - stock.adobe.com
Page 3: Flamingo Images - stock.adobe.com
Page 7: Jacob Lund - stock.adobe.com
Page 8: Gorodenkoff - stock.adobe.com
Page 11: simona - stock.adobe.com
Page 14: Astarot - stiock.adobe.com