April 2021

Business Basics

Dealing with data

fsb | Legal Protection Scheme

fsb.org.uk

Your guide to protecting data in your small business

All data or information that relates to an identifiable individual that your business stores or handles need to be properly protected. From financial information and payment details to contact information for your staff, personal data usage in the UK is protected by law.

Dealing with data is an ever-evolving matter in your business. Whether you're signing new contracts with suppliers, launching an email campaign or expanding your team, data protection and security should be a priority.

And, if you're looking to start your own business, it's helpful to prepare for data protection early in your business planning stage. This way you can hit the ground running without having to worry about any potential data compliance issues.

We'll delve into the world of data to explain what all small business owners and the self-employed need to keep in mind, answering the following frequently asked questions:

- What is the Data Protection Act?
- How can data protection affect a small business?
- What is personal data?
- What is a data protection officer? Do I need one?
- What is a data protection policy?
- I've received a data request – what do I do?
- How can I stay safe with third-party data?

What is the Data Protection Act?

Personal data usage in the UK is protected by law. The Data Protection Act 2018 along with the UK GDPR contain a set of principles that organisations, the public sector and businesses have to adhere to in order to keep someone's personal data accurate, safe, secure and lawful.

How can data protection affect a small business?

Small businesses handle personal data every day, from taking customer details for an order to filing staff records. You might not think you deal with much personal data, but you should be careful to ascertain what personal data you do hold, and should protect it accordingly.

Data protection law is in place to prevent personal data from being misused by organisations, for example illegal marketing purposes, and third parties for fraud, such as phishing scams and identity theft. Following proper data protection procedures is crucial to help prevent misuse and cybercrimes by ensuring personal details like banking, addresses and contact information - are protected.

A breach in your data defences can be costly, and in some cases affected customers and staff may pursue compensation against your business. You can also leave yourself open to punishment, as data breaches and non-compliance can put your business at risk of facing prosecution or fines.

The **Crown Prosecution Service** outlines several criminal offences under the law, including:

- Making a false statement in response to an information notice
- Destroying or falsifying information and documents
- Unlawfully obtaining personal data

What is personal data?

Personal data is generally information that relates to an identified or identifiable person, such as names, addresses and personal emails. Even if you cannot directly identify an individual purely from the data you hold, you still need to consider whether an individual may be identifiable if this data is put together with other information which may be held elsewhere.

Your business might store employee records, customer details or transactions. This data usually contains personal information that could relate to:

- your current staff and their partners or next of kin
- shareholders, business partners and clients
- customers and other members of the public

Whether you're recruiting new staff or marketing your freelance services, all personal data must be handled in accordance with the UK data protection rules. Examples of the key things to remember when you are handling personal data are:

- Only using it in specifically stated or relevant ways
- Not storing it for longer than you need to
- Keeping it safe and secure
- Storing it in line with data protection rights

You have a duty to ensure all information is correct and should confirm it's up to date with the party in question, such as when you're creating an employee record or signing customers up to a loyalty scheme.

What is a data protection officer? Do I need one?

Public authorities and businesses that do large scale monitoring or large-scale processing of certain types of data are required to appoint a designated data protection officer (DPO). However, this isn't a requirement for most small businesses.

Even though most small businesses do not need a data protection officer you could decide to hire a staff member to handle your data protection issues, but it might be more effective if you reshuffle your existing staff roles so that you have an employee dedicated to handling the majority of your business' data-related obligations. If you do decide to this, it's advisable to make sure they are properly trained and are fully aware of the different aspects.

If you're working alone, it's worth getting up to speed with your data responsibilities, especially if you're dealing with multiple clients at once.

What is a data protection policy?

It's recommended that your business should have a data protection policy which outlines how your business protects personal data, and it can also be used as evidence of your commitment to comply with the data protection legislation if you're ever investigated.

Your policy should include:

- Rules and guidelines on how you're complying with data protection laws
- Processes and procedures that any employees should follow
- Name and contact details of your data protection officer or member of staff who is responsible for data protection

Access your data protection paperwork toolkit

Don't start from scratch. From template data processing agreements and policies to DIY consent forms, privacy notices and letters, FSB members can save time with access to an online library of over 1,200 legal documents, guides and more.

I've received a data request – what do I do?

Data protection law gives anyone the right to ask if your business holds personal information about them in certain circumstances, including where it came from, why it's being used and who can see it.

You must:

- ☐ Respond as soon as possible and generally within 1 month
- ☐ Check the identity of the person who sent the request
- ☐ Provide confirmation that you're processing their personal data
- ☐ Provide a hard copy of the data (remove any data that doesn't relate to them)
- ☐ Give details about how their data is collected, used and disposed of
- ☐ Generally you should not charge a fee unless the request is manifestly unfounded or excessive

There are limited circumstances when you may not be required to comply either in full or partially, for example if disclosing the data would compromise the data of a 3rd party individual

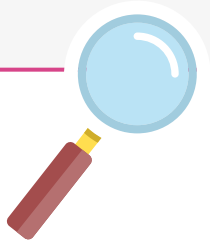
The ICO has detailed guidance and answers to frequently asked questions about rights of access.

How can I stay safe with third-party data?

If you rely on third parties – suppliers or service providers – to process your data, then you must check if they have appropriate security measures in place. Under the data protection rules, you're responsible for any personal data that is handled by third parties that contract with you.

When using third-party data, much of your data security risks may be in the hands of others. You need to understand these risks and be confident that appropriate measures are in place to protect your business and your customers.

Identify all current and potential suppliers or service providers



Ask the right questions to assess their data and cyber security measures

For example:

Do they have Cyber Essentials certification? Do they maintain data and cyber security policies? What are their incident response plans? How do they control access to their data?

Have a contract in place which sets out the third-party's obligations with regard to the data they are processing on your behalf

Choose your partners with data protection in mind

If you have any concerns, you should insist on action before engaging with them

Call FSB's 24/7 legal advice line if you have any questions

Keeping your data secure

Of course, the ideal scenario is to prevent data breaches or offences in the first instance. Ensuring you adhere to data protection policies is crucial as the effects of non-compliance can be devastating for you and your business. Clear processes, policies and training on data protection compliance can help to mitigate the risks.

However, if you find yourself subject to data protection prosecution, we've got you covered. Our data protection prosecution cover includes legal representation for defending legal proceedings brought by the Registrar or appeals against the refusal of an application or Enforcement Notice.

Additional resources

Take a deeper dive into data protection with these resources.

- The Information Commissioner's Office has detailed guidance for small businesses
- Check the Government website for more information on data protection rules and the law on marketing and advertising
- ICO's guide to Data Protection Impact Assessments (DPIAs)