Getting ready for the new UK data protection law

Eight practical steps for micro business owners and sole traders

ico.
Information Commissioner's Office

1. **Know** the law is changing – which you now do, so that's one thing you've done already!

2. **Make sure you have a record** of the personal data you hold and why.

3. **Identify** why you have personal data and how you use it.

4. **Have a plan** in case people ask about their rights regarding the personal information you hold about them.

5. **Ask yourself: before I collect their data**, do I clearly tell people why I need it and how I will use it?

6. **Check your security.** This can include locking filing cabinets and password-protecting any of your devices and cloud storage that hold your staff or customers' personal data.

7. **Develop a process** to make sure you know what to do if you breach data protection rules.

8. **Don't panic: we're here to help.** For example, you can click here to see some frequently asked questions and their answers for several different business sectors.

DATA PROTECTION

Make it your business at **ico.org.uk**

Eight practical steps for micro business owners and sole traders getting ready for the new UK data protection law

ico.
Information Commissioner's Office

Any business that handles personal data, even micro-businesses with fewer than ten staff, will have to follow new data protection rules from 25 May 2018.

Many members of the public are demanding higher standards from organisations – large and small – that collect and use their personal information.

Following these steps will help you comply with the law and give your customers what they increasingly expect.

If you already have policies and procedures to help you comply with current data protection law, you are in a good position. However, you will have to do some things for the first time, or do them differently, from 25 May.

DATA PROTECTION

Make it your business at **ico.org.uk**

Step 1:
Know the law is changing

1 **You also need to make sure all your employees know the law is changing.**

You then need to:

- understand how this change could affect your business, and
- identify anything you need to alter to comply with the law.

Step 2:
Keep a record of the personal data you hold and why

ico.
Information Commissioner's Office

2

You need to keep records of the personal data you hold and work with. This means recording information including:

- the personal data you hold – eg names, emails, individuals' financial information
- how you got this information – eg a customer form, bought-in marketing lists, staff application forms
- why you have this information
- how long you've had it
- whether you still need it – if not, this is an opportunity to delete it
- if you share this information with other organisations, or
- if the information you have is 'special category data'. Examples include health records or information about someone's race, religion or sexual orientation.

Step 3:
Identify why you have personal data and how you use it

ico.
Information Commissioner's Office

3

You have to identify your reason for collecting and handling personal data. This will help you identify your 'lawful basis' for processing personal data under the new law.

There are six available lawful bases for processing personal data. None of them is stronger or more important than the others. The most appropriate basis to use will depend on the reason for processing the personal data and your relationship with the individual – eg are they a customer or employee? You must keep a record of your lawful basis and update your privacy information (see step 5) to explain it.

You will also have to explain your lawful basis if a person asks for a copy of all the information you have about them (see step 4 – right to access).

We are creating a tool to help organisations identify their lawful basis. This will be ready before 25 May 2018.

Step 4:
Have a plan in case people ask about the rights they have regarding the personal data you hold about them

4

Under the new law, people have the following data protection rights:

The right to be informed
Individuals have the right to know why and how their personal data is being processed. Having a good privacy notice (see step 3) will help make sure you're protecting this right. Further Information

The right of access
Under current data protection law, people already have the right to ask you for a copy of all the information you hold about them. This is called a subject access request.

The right of individuals to access their personal data will still exist under the new law. So, before 25 May 2018, make sure you have processes in place that allow you to provide this information to the individual making the request. Under the new law you'll need to provide the information within one month.

A copy of the requested information must be provided to the individual free of charge unless the request is what the law calls 'manifestly unfounded or excessive', in particular if it is repetitive. If you decide to charge a fee, it must be based on the administrative cost of providing the information.

If you refuse, you must tell the person why and let them know they can complain to the ICO or seek a judicial remedy. You have to do this as soon as possible and within one month. Further Information

The right to rectification
Individuals have the right to have their information corrected if they believe it is factually inaccurate – this is known as the right to rectification.

For example, if a builder sends an invoice to a customer at the wrong home address, they should change the address once they are told it is wrong and have been given the correct details. If the builder shared the incorrect information with another organisation, it is up to the builder to try to ensure that the other company is aware of the correction to the information. The builder must inform the other organisation unless this proves impossible or involves disproportionate effort. Further Information

Step 4:
Have a plan in case people ask about the rights they have regarding the personal data you hold about them

ico.
Information Commissioner's Office

4

The right to erasure
The right to erasure is also known as 'the right to be forgotten'. In certain circumstances, it allows people to instruct organisations to delete or remove their personal data.

For example, a website holds photographs of a drunken young person in fancy dress, and 20 years later the photo is stopping them getting a job. The individual can ask for the picture to be deleted.

If you receive a request for the deletion or removal of personal data, you must consider the grounds for the request and decide whether you should comply or whether the law allows you to refuse. Further Information

The right to restriction of processing
In certain circumstances, individuals have a right to stop businesses processing their personal data. Where this right applies (eg if the individual contests the accuracy of the data or the processing is unlawful), you are still allowed to store the personal data but must not use it for any other purposes unless certain conditions apply. In most cases the restriction will not be in place forever, but for a limited time; for example while you consider the accuracy of the data or review whether you have legitimate grounds to override the objection. Further Information

The right to data portability
This is a new right that lets people get hold of and re-use their personal data for their own benefit across different services. It applies:

- to personal data a person has given you, and
- when you are processing that data on the basis of consent or for the performance of a contract (see step 3), and
- when the data is being processed by automated means.

For example, a customer wants to change their mobile phone provider and port their call and bill history to a new provider. They have the right to instruct their current provider to transport their personal data to the new company in a commonly used electronic format. Further Information

The right to object
Individuals have the right to object to the processing of their personal data for several reasons. In particular, you may receive an objection to your business sending direct marketing to a customer. If this happens, you must stop using their personal data for any direct marketing purposes.

You can find more information on individuals' rights under the new law, and the circumstances in which they apply, in our Guide to the GDPR. Further Information

Step 5:
Before you collect their personal data, do you clearly tell people why you need it and how you will use it?

ico.
Information Commissioner's Office

5

At the point you collect personal data from people, you must provide them with certain information, including the identity of your business and how you plan to use their information. You need to do this so your customers, employees and other individuals understand what you will do with the personal data you collect. Under the new law, you have to explain your lawful basis for processing personal data (see step 3).

You also need to tell people about their rights (see step 4) and their ability to complain to the ICO if they are concerned about how you handle their information. Your privacy notices must be easy to understand and given to individuals whenever you collect their personal data, both online and offline.

Step 6:
Check your security

6

This can include locking filing cabinets and password-protecting any of your devices and cloud storage that hold your staff or customers' personal information.

You must ensure that personal data is held securely. This includes protecting data against unauthorised or illegal use and against accidental loss, destruction or damage.

Steps you can take to protect the personal data you hold include:

- password-protecting and encrypting your electronic devices
- pseudonymisation (the use of made-up names)
- setting up firewalls
- installing anti-virus software
- securing your business premises, and
- using securely locked storage for paper records.

To find out more about securing your IT systems, you can read our practical guide to IT security.

Step 7:
Develop a process to make sure you know what to do if you break data protection rules

7

For example, if the breach is likely to result in damage to a person's reputation, financial loss, loss of confidentiality, or major financial or social disadvantage, you should notify the ICO.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, you should also contact them directly and without undue delay.

You should start to think about the possible breaches that could occur in your business, for example:

- paperwork or IT devices are lost or stolen
- malware is used to gain access to your computer systems
- personal data is sent to the wrong person by email, post or fax, or
- documents are not disposed of properly, eg not shredded.

You should also think about how you would identify that a breach had occurred, and its possible impacts on the people whose data had been affected.

If you are unsure whether you have suffered a data breach or if you need to report a breach to the ICO, then please call our dedicated personal data breach helpline on 0303 123 1113 option B.

You should then think about how you would know if a breach had happened and what the impact would be on the people whose data had been affected.

If you are unsure if you have had a data breach or if you need to report it to the ICO, then please call our dedicated personal data breach helpline on 0303 123 1113

Step 8:
Do not panic

ico.
Information Commissioner's Office

8

Some of the information and news you may have seen about the new law from sources outside the ICO has been inaccurate or misleading. Inaccurate information has resulted in organisations becoming increasingly worried about the coming changes. For example, you may have seen statements along these lines:

"GDPR will stop dentists ringing patients to remind them about appointments." This is wrong!

"Cleaners and gardeners will face massive fines that will put them out of business." This is wrong!

"All breaches must be reported under GDPR." This is wrong!

A common myth is that the ICO will be fining organisations large sums for every breach of data protection law. Please remember: the ICO is here to uphold the information rights of the UK public. We can and do fine organisations, but we have other tools at our disposal to ensure that businesses comply with the law. Monetary penalties have been and will continue to be a last resort of our regulatory action – our primary aim is to support businesses to get things right and improve their practices where required.
