

Introduction to data protection	2
Some basic concepts	3
About the DPA 2018	7
Which regime?	10

Introduction to data protection

This section of our [Guide to Data Protection](#) introduces some basic data protection concepts and explains how the Data Protection Act 2018 (DPA 2018) works.

It will help you understand the legal framework. It does not contain guidance on how to comply in practice – that is for the other sections of this guide - but it will help you identify which sections of the guide to read.

If you already know which part of the DPA 2018 applies to you, you can go straight to the relevant section of the guide for practical guidance on how to comply. For most organisations, this will be the [Guide to the UK GDPR](#).

Some basic concepts

At a glance

- Data protection is about ensuring people can trust you to use their data fairly and responsibly.
- If you collect information about individuals for any reason other than your own personal, family or household purposes, you need to comply.
- The UK data protection regime is set out in the DPA 2018, along with the UK GDPR. It takes a flexible, risk-based approach which puts the onus on you to think about and justify how and why you use data.
- The ICO regulates data protection in the UK. We offer advice and guidance, promote good practice, carry out audits, consider complaints, monitor compliance and take enforcement action where appropriate.

In brief

- [What is data protection?](#)
- [Does it apply to me?](#)
- [Why don't you tell me exactly what to do?](#)
- [What is 'personal data'?](#)
- [What is 'processing'?](#)
- [What is a 'controller'?](#)
- [What is a 'processor'?](#)
- [What is a 'data subject'?](#)
- [What is the ICO's role?](#)

What is data protection?

Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

It's also about removing unnecessary barriers to trade and co-operation. It exists in part because of international treaties for common standards that enable the free flow of data across borders. The UK has been actively involved in developing these standards.

Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

The UK data protection regime is set out in the DPA 2018 and the UK GDPR.

Does it apply to me?

Yes, if you have information about people for any business or other non-household purpose. The law applies to any 'processing of personal data', and will catch most businesses and organisations, whatever their size.

You will not need to comply if you only use the information for your own personal, family or household purposes – eg personal social media activity, private letters and emails, or use of your own household gadgets.

Why don't you tell me exactly what to do?

Every organisation is different and there is no one-size fits-all answer. Data protection law doesn't set many absolute rules. Instead it takes a risk-based approach, based on some key principles. This means it's flexible and can be applied to a huge range of organisations and situations, and it doesn't act as a barrier to doing new things in new ways.

However, this flexibility does mean that you need to think about - and take responsibility for - the specific ways you use personal data. Whether and how you comply depends on exactly why and how you use the data - and there is often more than one way to comply.

This guide includes examples, checklists and other tools to help you ask the right questions, and understand your options. However, you know your organisation best, so it's up to you to decide on – and be able to justify – your answers. This is a key principle of data protection law, known as the accountability principle.

What is 'personal data'?

In short, personal data means information about a particular living individual. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public.

It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

It doesn't cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.

It only includes paper records if you plan to put them on a computer (or other digital device) or file them in an organised way. If you are a public authority, all paper records are technically included – but you will be exempt from most of the usual data protection rules for unfiled papers and notes.

Further reading – Guide to the UK GDPR

We have [more guidance on what is personal data](#) in the Guide to the UK GDPR key definitions section.

What is 'processing'?

Almost anything you do with data counts as processing; including collecting, recording, storing, using,

analysing, combining, disclosing or deleting it.

What is a 'controller'?

A controller is the person that decides how and why to collect and use the data. This will usually be an organisation, but can be an individual such as a sole trader, partner in an unincorporated partnership, or self-employed professional, eg a barrister. If you are an employee acting on behalf of your employer, the employer would be the controller. The controller must make sure that the processing of that data complies with data protection law.

In this guide, we generally use the term 'organisation' or 'you' to mean the controller.

What is a 'processor'?

A processor is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

Further reading – Guide to the UK GDPR

We have [more guidance on controllers and processors](#) in our Guide to the UK GDPR key definitions section.

What is a 'data subject'?


This is the technical term for the individual whom particular personal data is about. In this guide we generally use the term 'individuals' instead.


What is the ICO's role?

The ICO regulates data protection in the UK. We offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.

We also cooperate with data protection authorities in other countries, including the European Data Protection Board (EDPB), which includes representatives from data protection authorities in each EU member state.

Further Reading

 [What we do](#)
About the ICO

 [Action we've taken](#)
Action we've taken

About the DPA 2018

At a glance

- The DPA 2018 sets out the data protection framework in the UK, alongside the UK GDPR. It contains three separate data protection regimes:
 - Part 2: sets out a general processing regime (the UK GDPR);
 - Part 3: sets out a separate regime for law enforcement authorities; and
 - Part 4: sets out a separate regime for the three intelligence services.

In brief

- [What is the DPA 2018?](#)
- [What is the UK GDPR?](#)
- [How does the DPA 2018 work?](#)
- [What is the general processing regime?](#)
- [What is the law enforcement processing regime?](#)
- [What is the intelligence services processing regime?](#)
- [Which regime applies?](#)

What is the DPA 2018?

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

It sits alongside and supplements the UK GDPR - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

The 'applied GDPR' provisions (that were part of Part 2 Chapter 3) enacted in 2018 were removed with effect from 1 Jan 2021 and are no longer relevant. The processing of manual unstructured data and processing for national security purposes now fall under the scope of the UK GDPR regime.

What is the UK GDPR?

The UK GDPR is the [UK General Data Protection Regulation](#). It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR ([General Data Protection Regulation \(EU\) 2016/679](#)) which applied in the UK before that date, with some changes to make it work more effectively in a UK context,

You may need to comply with both the UK GDPR and the EU GDPR if you operate in Europe, offer goods or

services to individuals in Europe, or monitor the behaviour of individuals in Europe. The EU GDPR is regulated separately by European supervisory authorities, and you may need to seek your own legal advice on your EU obligations.

If you hold any overseas data collected before 01 January 2021 (referred to as 'legacy data'), this will be subject to the EU GDPR as it stood on 31 December 2020 (known as 'frozen GDPR'). In the short term, there is unlikely to be any significant change between the frozen GDPR and the UK GDPR.

Further reading

We have produced more guidance and resources on [Data protection and the end of the transition period](#).

How does the DPA 2018 work?

The DPA 2018 is split into a number of different parts, which apply in different situations and perform different functions. It sets out three separate data protection regimes:

- Part 2: General processing (UK GDPR);
- Part 3: Law enforcement processing; and
- Part 4: Intelligence services processing.

The other parts contain provisions of general application, including interpretation and our functions and powers. When using the DPA 2018 it is important to be clear which set of provisions apply.

Further reading

Before the changes made under the EU Withdrawal Act, we published [an overview of the DPA 2018](#) with a more detailed summary of its structure and content. This may still be useful if you need help navigating the legislation, but please be aware that there have been some changes (in particular the previous GDPR and applied GDPR chapters have now been merged to form the UK GDPR regime). We will consider whether to publish an updated version of this document in due course.

For more guidance on how the provisions work in practice, you should continue to read this Guide.

What is the general processing regime?

Part 2 of the DPA 2018 supplements and tailors the UK GDPR. For most organisations, this is the part that will apply. You need to read it alongside the UK GDPR itself, as both sets of provisions apply directly to you. The key provisions of this part are:

- sections 1-28;
- schedule 1 (conditions for processing some sensitive types of data);
- schedules 2-4 (exemptions); and

- schedule 21 (transitional provisions)

Further reading – ICO guidance

For more on how these provisions work in practice, read our [Guide to the UK GDPR](#).

What is the law enforcement processing regime?

Part 3 of the DPA 2018 sets out a separate data protection regime for authorities with law enforcement functions when they are processing for law enforcement purposes. It also applies to their processors.

The relevant provisions are:

- sections 29-81; and
- schedules 7-8.

Further reading – ICO guidance

For more on how these provisions work in practice, read our [Guide to law enforcement processing](#).

What is the intelligence services processing regime?

Part 4 of the DPA 2018 sets out a separate data protection regime for the intelligence services - MI5, SIS (sometimes known as MI6), and GCHQ – and their processors. The relevant provisions are:

- sections 82-113; and
- schedules 9-11.

Further reading – ICO guidance

For guidance on how these provisions work in practice, read our [Guide to intelligence services processing](#) (which is currently being developed).

Which regime applies?

Identifying the correct regime is important, as although the overall principles are similar, there are some key differences. You will need to be able to demonstrate that you are applying the correct regime.

Most organisations fall under the general processing regime and should read our [Guide to UK GDPR](#).

If you're not sure, click to the next page for more guidance to help you decide.

Which regime?

At a glance

- Most organisations fall under the general processing regime. Go to our [Guide to the UK GDPR](#).
- If you are a 'competent authority' with law enforcement functions and you are processing for law enforcement purposes, or you are a processor acting on their behalf, you fall under the law enforcement regime. Go to our [Guide to law enforcement processing](#).
- If you are a 'competent authority' processing for other non-law enforcement purposes, you fall under the general processing regime. Go to our [Guide to the UK GDPR](#).
- If you are one of the three UK intelligence services, or a processor acting on their behalf, you fall under the intelligence services regime. Go to our [Guide to intelligence services processing](#).

How do I decide which regime applies?

This self assessment tool can help you determine the data protection regime that applies to the data you process, now the UK's transition period from the EU has ended.

[Start now →](#)