Guide to data protection

ico.
Information Commissioner's Office

About the Guide to Data Protection

This guide is for data protection officers and others who have day-to-day responsibility for data protection. It is aimed at small and medium-sized organisations, but it may be useful for larger organisations too.

If you are a sole trader (or similar small business owner), you may find it easier to start with our specific resources for small business owners and sole traders.

The guide covers the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK. It is split into five main sections:

Introduction to data protection

This section introduces some basic concepts, explains how the DPA 2018 works, and helps you understand which parts apply to you. It will also help you identify which sections of this guide to read.

Guide to the GDPR

This section explains the GDPR as it applies in the UK, tailored by the DPA 2018. This section will be most relevant to most organisations.

Guide to Law Enforcement Processing

This section is for public authorities processing for law enforcement purposes.

Guide to Intelligence Services Processing

This section is for the three intelligence agencies: MI5, SIS (also known as MI6) and GCHQ.

Key data protection themes

This section contains guidance on key themes, explains how the law applies in that context, and links to any statutory codes of practice.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance, statutory ICO codes of practice, and European guidelines published by the European Data Protection Board (EDPB).

Other resources

Making data protection your business - resources for sole traders
For organisations

Data protection self assessment toolkit
For organisations

Archived data protection guidance on the old Data Protection Act 1998

For organisations

We produced many guidance documents on the previous 1998 Act. Even though that Act is no longer in force, some of this guidance contains practical examples and advice which may still be helpful in applying the new legislation. While we are developing our new guidance we will keep those documents accessible on our website, with the proviso that they cannot be taken as guidance on the DPA 2018.

What's new?

We will update this page to highlight and link to what's new in our Guide to Data Protection.

September 2019

We have published guidance on manifestly unfounded and excessive requests under the Guide to Law Enforcement Processing.

August 2019

We have updated our position on how to calculate the time limit for responding to requests (in relation to Individual rights) following a determination made in a Court of Justice of the European Union (CJEU) case which has been adopted by the European Data Protection Board (EDPB). We have also added guidance on the meaning of 'manifestly unfounded or excessive'. The following pages have been updated:

- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to data portability; and
- Right to object.

June 2019

The European Data Protection Board (EDPB) published Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects for consultation. The consultation closed on 24 May.

We have updated the page in the lawful basis section on contract and the lawful basis tool to reflect the Guidelines.

March 2019

The European Data Protection Board (EDPB) has adopted:

- Guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.
- Guidelines on the accreditation of certification bodies under Article 43 of the GDPR (2016/679).

The EDPB has also published the following Guidelines for consultation:

- Guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 – Annex 2 – closing 29 March 2019.
- Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 – closing 2 April

2019.

Comments should be sent to EDPB@edpb.europa.eu.

We've also updated our guidance on the Right to be Informed.

December 2018

We have published our Guide to Data Protection, combining our existing guidance on the GDPR and law enforcement regimes with new guidance explaining some basic concepts, how the DPA 2018 works, and which regime applies.

We have expanded our guidance on scope and key definitions in the guide to law enforcement processing.

We have expanded our guidance on contracts, published guidance on controllers and processors and published detailed guidance on controllers and processors and contracts and liabilities.

November 2018

We have published detailed guidance on encryption.

September 2018

We have expanded our guidance on Exemptions.

August 2018

We have expanded our guidance on International transfers.

May 2018

The European Data Protection Board (EDPB) has published draft guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 for consultation. The consultation will end on 12 July.

We have published detailed guidance on children and the GDPR.

We have published detailed guidance on determining what is personal data.

We have expanded our guidance on data protection by design and default, and published detailed guidance on automated decision-making and profiling.

We have published a new page on codes of conduct, and a new page on certification.

We have published detailed guidance on the right to be informed.

We have published detailed guidance on Data Protection Impact Assessments (DPIAs).

We have expanded the pages on the right of access and the right to object.

We have published detailed guidance on consent.

We have expanded the page on the right to data portability.

April 2018

We have expanded the page on Accountability and governance.

We have expanded the page on Security.

We have updated all of the lawful basis pages to include a link to the lawful basis interactive guidance tool.

March 2018

We have published detailed guidance on DPIAs for consultation. The consultation will end on 13 April 2018. We have also updated the guide page on DPIAs to include the guide level content from the detailed guidance.

We have published detailed guidance on legitimate interests.

We have expanded the pages on:

- Data protection impact assessments
- Data protection officers
- The right to be informed
- The right to erasure
- The right to rectification
- The right to restrict processing

February 2018

The consultation period for the Article 29 Working party guidelines on consent has now ended and comments are being reviewed. The latest timetable is for the guidelines to be finalised for adoption on 10-11 April.

The consultation period for the Article 29 Working Party guidelines on transparency has now ended.

Following the consultation period, the Article 29 Working Party has adopted final guidelines on Automated individual decision-making and Profiling and personal data breach notification. These have been added to the Guide.

We have published our Guide to the data protection fee.

We have updated the page on Children to include the guide level content from the detailed guidance on Children and the GDPR which is out for public consultation.

January 2018

We have published more detailed guidance on documentation.

We have expanded the page on personal data breaches.

We have also added four new pages in the lawful basis section, covering contract, legal obligation, vital interests and public task.

December 2017

We have published detailed guidance on Children and the GDPR for public consultation. The consultation closes on 28 February 2018.

The sections on Lawful basis for processing and Rights related to automated individual decision making including profiling contain new expanded guidance. We have updated the section on Documentation with additional guidance and documentation templates. We have also added new sections on legitimate interests, special category data and criminal offence data, and updated the section on consent.

The Article 29 Working Party has published the following guidance, which is now included in the Guide.

- Consent
- Transparency

It is inviting comments on these guidelines until 23 January 2018.

The consultation for the Article 29 Working Party guidelines on breach notification and automated decision-making and profiling ended on 28 November. We are reviewing the comments received together with other members of the Article 29 Working Party and expect the guidelines to be finalised in early 2018.

November 2017

The Article 29 Working Party has published guidelines on imposing administrative fines.

We have replaced the Overview of the GDPR with the Guide to the GDPR. The Guide currently contains similar content to the Overview, but we have expanded the sections on Consent and Contracts and Liabilities on the basis of the guidance on these topics which we have previously published for consultation.

The Guide to the GDPR is not yet a finished product; it is a framework on which we will build upcoming GDPR guidance and it reflects how future GDPR guidance will be presented. We will be publishing more detailed guidance on some topics and we will link to these from the Guide. We will do the same for guidelines from the Article 29 Working Party.

October 2017

The Article 29 Working Party has published the following guidance, which is now included in our overview.

- Breach notification
- Automated individual decision-making and Profiling

The Article 29 Working Party has also adopted guidelines on administrative fines and these are expected to be published soon.

In the Rights related to automated decision making and profiling we have updated the next steps for the ICO.

In the Key areas to consider we have updated the next steps in regard to the ICO's consent guidance.

The deadline for responses to our draft GDPR guidance on contracts and liabilities for controllers and processors has now passed. We are analysing the feedback and this will feed into the final version.

September 2017

We have put out for consultation our draft GDPR guidance on contracts and liabilities for controllers and processors.

July 2017

In the Key areas to consider we have updated the next steps in regard to the ICO's consent guidance and the Article 29 Working Party's Europe-wide consent guidelines.

June 2017

The Article 29 Working Party's consultation on their guidelines on high risk processing and data protection impact assessments closed on 23 May. We await the adoption of the final version.

May 2017

We have updated our GDPR 12 steps to take now document.

We have added a Getting ready for GDPR checklist to our self-assessment toolkit.

April 2017

We have published our profiling discussion paper for feedback.

March 2017

We have published our draft consent guidance for public consultation.

January 2017

Article 29 have published the following guidance, which is now included in our overview:

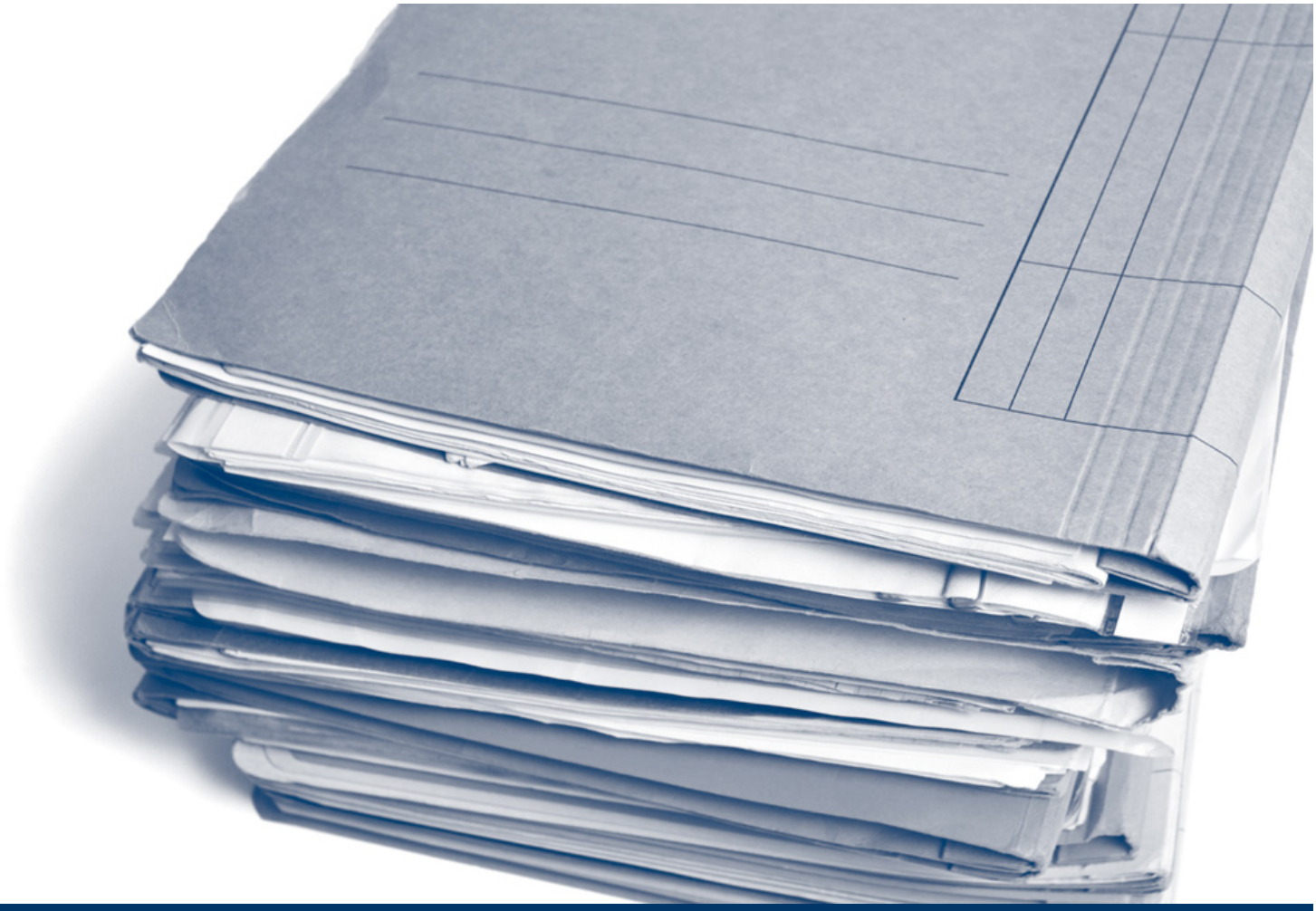
- Data portability
- Lead supervisory authorities
- Data protection officers

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 GDPR.



Introduction to DPA 2018

Click here to read the Introduction to data protection.

Guide to the GDPR

The Guide to the GDPR is part of our Guide to Data Protection. It is for DPOs and others who have day-to-day responsibility for data protection.

It explains the general data protection regime that applies to most UK businesses and organisations. It covers the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018.

It explains each of the data protection principles, rights and obligations. It summarises the key points you need to know, answers frequently asked questions, and contains practical checklists to help you comply.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance, statutory ICO codes of practice, and European guidance published by the European Data Protection Board (EDPB).

Guide to the General Data Protection Regulation (GDPR)

Click here to read the Guide to the GDPR.

Guide to Law Enforcement Processing

The Guide to Law Enforcement Processing is part of our Guide to Data Protection. It is for those who have day-to-day responsibility for data protection in organisations with law enforcement functions.

It explains the data protection regime that applies to those authorities when processing personal data for law enforcement purposes. It covers part 3 of the Data Protection Act 2018 (DPA 2018), which implements an EU Directive (Directive 2016/680) and is separate from the GDPR regime.

It explains each of the data protection principles, rights and obligations. It summarises the key points you need to know and answers frequently asked questions.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance and European guidance published by the European Data Protection Board (EDPB).

This section only covers processing for law enforcement purposes. You will need to read our Guide to the GDPR when processing for non-law enforcement purposes.

Guide to Law Enforcement Processing

Click here to read the Guide to Law Enforcement Processing.

Guide to Intelligence Services Processing

This section of our Guide to Data Protection is only relevant for the intelligence services - MI5, SIS (commonly known as MI6) and GCHQ - or for processors acting on their behalf.

We are currently developing our guidance on the separate data protection regime that applies to these intelligence services. It will cover the provisions in part 4 of the Data Protection Act 2018 (DPA 2018).

It will explain each of the data protection principles, rights and obligations. It will summarise the key points, answer frequently asked questions, and include practical checklists.

This section will expand once our guidance is finalised.

Key data protection themes

This section of our Guide to Data Protection contains guidance on key themes and topics, explaining how the law applies in a specific context. It is for data protection officers and others who have day-to-day responsibility for data protection.

It covers the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK.

We are currently developing guidance or statutory codes of practice on a number of key themes, including children's data, age-appropriate design, marketing, political campaigning, data sharing, journalism, national security, and various technologies. This section will expand over time as our work develops.

Each page summarises the key points you need to know, answers frequently asked questions, and contains practical checklists to help you comply.

Where relevant, we also link to statutory codes of practice, detailed guidance and other resources, including European guidance published by the European Data Protection Board (EDPB).

Key data protection themes

Click here to read the guide on Key data protection themes.