

Data sharing

code of practice

Information Commissioner’s foreword	3
Executive summary	5
Navigating the data sharing code	7
About this code	10
Data sharing covered by the code	19
Deciding to share data	23
Data sharing agreements	26
Data protection principles	30
Accountability	31
Fairness and transparency in data sharing	35
Lawfulness	37
Lawful basis for sharing personal data	41
Security	44
The rights of individuals	46
Law enforcement processing	51
Due diligence	57
Sharing personal data in databases and lists	59
Data sharing and children	62
Data sharing in an urgent situation or in an emergency	64
Data sharing across the public sector: the Digital Economy Act codes	66
Enforcement of this code	68
Glossary	71
Annex A: data sharing checklist	75
Annex B: Data sharing request form template	79
Data sharing decision form template	81
Annex C: case studies	84

# Information Commissioner's foreword

The UK Government has laid the Data Sharing Code of Practice before Parliament on 18 May 2021. It will lay before Parliament for 40 sitting days before coming into force.

## Information Commissioner's foreword

In 2011 the ICO published its first Data Sharing Code; in the intervening period the type and amount of data collected by organisations has changed enormously, as has the technology used to store and share it, and even the purposes for which it is used. It is imperative that we keep up to date with these developments through this new code.

As the UK Information Commissioner, I know that data is one of modern society's greatest assets. Ready access to information and knowledge, including about individual citizens, can lead to many economic and social benefits, including greater growth, technological innovations and the delivery of more efficient and targeted services.

We have written this Data Sharing Code to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way in this changing landscape. This code will guide practitioners through the practical steps they need to take to share data while protecting people's privacy. We hope to dispel many of the misunderstandings about data sharing along the way.

I have seen first-hand how proportionate, targeted data sharing delivered at pace between organisations in the public, private and voluntary sectors has been crucial to supporting and protecting the most vulnerable during the response to the COVID-19 pandemic. Be it through the shielding programme for vulnerable people, or sharing of health data in the Test and Trace system. On a local and national level, data sharing has been pivotal to fast, efficient and effective delivery of pandemic responses.

Utilising the data we collectively hold and allowing it to be maximised properly will have economic benefits. Data sharing that engenders trust in how personal data is being used is a driver of innovation, competition, economic growth and greater choice for consumers and citizens. This is also true in the sphere of public service delivery where efficient sharing of data can improve insights, outcomes and increase options for recipients.

This code demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist. But we cannot pretend that a code of practice is a panacea to solve all the challenges for data sharing. Or that targeted ICO engagement and advice will solve everything. There are other barriers to data sharing, including cultural, technical and organisational factors. Overcoming these will require more than just the ICO; it will require a collective effort from practitioners, government and the regulator.

I see the publication of this code not as a conclusion but as a milestone in this ongoing work. The ICO will continue to provide clarity and advice in how data can be shared in line with the law. This code, and the products and toolkits published alongside it, provides a gateway to good data sharing practice and the benefits we can expect from the results.

Elizabeth Denham CBE

Information Commissioner

# Executive summary

## About this code

- This is a statutory code of practice made under section 121 of the Data Protection Act 2018.
- It is a practical guide for organisations about how to share personal data in compliance with data protection law. It aims to give you confidence to share data fairly and proportionately.

## Data protection law enables fair and proportionate data sharing

- Data protection law facilitates data sharing when you approach it in a fair and proportionate way.
- Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker. It provides a framework to help you make decisions about sharing data.
- This code helps you to balance the benefits and risks and implement data sharing.
- Data sharing has benefits for society as a whole.
- Sometimes it can be more harmful not to share data.
- When considering sharing data:
  - you must comply with data protection law;
  - we recommend that you assess the risks using a Data Protection Impact Assessment (DPIA); and
  - it is good practice to have a data sharing agreement.
- When sharing data, you must follow the key principles in data protection legislation:
  - The accountability principle means that you are responsible for your compliance, and you must be able to demonstrate that compliance.
  - You must share personal data fairly and transparently.
  - You must identify at least one lawful basis for sharing data before you start any sharing.
  - You must process personal data securely, with appropriate organisational and technical measures in place.
- In your data sharing arrangement, you should have policies and procedures that allow data subjects to exercise their individual rights easily.
- You can share data in an emergency, as is necessary and proportionate. Examples of an emergency situation are the risk of serious harm to human life, or the immediate need to protect national security.
- You may share children's data if you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
- The government has devised a framework for the sharing of personal data, for defined purposes across the public sector, under the Digital Economy Act 2017 (DEA).

## UK exit from the European Union

- Now the UK has left the EU, the GDPR (which we refer to in this code as the EU GDPR) has been written

into UK law as the UK GDPR, to sit alongside the DPA 2018.

- For the latest information and guidance on data protection and the UK's position in relation to data protection and the EU, see the ICO website.

## ICO powers

- The ICO upholds information rights in the public interest. Our focus is to help you carry out data sharing in a compliant way. We will always use our powers in a targeted and proportionate manner, in line with our regulatory action policy.

# Navigating the data sharing code

A quick reference guide to help you find the content you need on each topic.

What you need to do or consider		Where you can find it in the data sharing code
<b>Identify your objective in sharing the data</b>		<ul style="list-style-type: none"><li>• <a href="#">Deciding to share data</a></li><li>• <a href="#">Data sharing agreements</a></li></ul>
<b>Be clear as to what data you are sharing</b>		<ul style="list-style-type: none"><li>• <a href="#">Deciding to share data</a></li><li>• <a href="#">Data sharing agreements</a></li></ul>
<b>Understand the position following UK exit from the EU</b>		<ul style="list-style-type: none"><li>• <a href="#">How is this code affected by the UK's exit from the European Union?</a></li></ul>
<b>Consider the benefits and risks of sharing and not sharing</b>		<ul style="list-style-type: none"><li>• <a href="#">What is the purpose of this code?</a></li><li>• <a href="#">The benefits of data sharing</a></li><li>• <a href="#">Deciding to share data</a></li></ul>
<b>Carry out a Data Protection Impact Assessment (DPIA)</b>		<ul style="list-style-type: none"><li>• <a href="#">Deciding to share data</a></li></ul>
<b>Put in place a data sharing agreement</b>		<ul style="list-style-type: none"><li>• <a href="#">Data sharing agreements</a></li><li>• <a href="#">Accountability</a></li></ul>

**Ensure you follow the data protection principles**



- [Data protection principles](#)

**Check your data sharing is fair and transparent**



- [Fairness and transparency](#)

**Identify at least one lawful basis for sharing the data before you start sharing it**



- [What is our lawful basis for sharing?](#)
- [Lawful basis for sharing personal data](#)

**Put in place policies and procedures that allow data subjects to exercise their individual rights easily**



- [What about access and individual rights?](#)
- [The rights of individuals](#)
- [Law enforcement processing](#)

**Be clear about sharing data under the law enforcement processing provisions of Part 3 DPA 2018, and sharing between the UK GDPR/Part 2 DPA 2018 and Part 3 DPA 2018**



- [Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR and Part 2 DPA 2018](#)

**Demonstrate a compelling reason if you are planning to share children's data, taking account of the best interests of the child**



- [Data sharing and children](#)

**Share data in an emergency as is necessary and proportionate. Plan ahead as far as possible**



- [Data sharing in an urgent situation or in an emergency](#)

**Document your decisions about the data sharing, evidencing your compliance with data protection law**



- [Accountability](#)
- [Data sharing agreements](#)



**Put in place quality checks on the data**



- [What information governance arrangements should we have?](#)

**Arrange regular reviews of the data sharing arrangement**



- [When should we review a data sharing arrangement?](#)
- [Accountability](#)

**Agree retention periods and make arrangements for secure deletion**



- [Security](#)
- [Accountability](#)

# About this code

## At a glance

This is a statutory code of practice prepared under section 121 of the Data Protection Act 2018.

It is a practical guide for organisations about how to share personal data in a way that complies with data protection law.

It aims to give you confidence to share data fairly and proportionately.

## In more detail

- [What is the status of this code?](#)
- [How is this code affected by the UK's exit from the European Union?](#)
- [What happens if we don't comply with the code?](#)
- [What is the purpose of this code?](#)
- [Who is this code for?](#)
- [Common misconceptions about data sharing](#)
- [How should we use the code?](#)

## What is the status of this code?

This is a statutory code of practice prepared under section 121 of the Data Protection Act 2018 (DPA 2018):



"The Commissioner must prepare a code of practice which contains—

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data."

It was laid before Parliament on [date] and issued on [date], under section 125 of the DPA 2018. It comes into force on [date].

The code contains practical guidance on how to share data fairly and lawfully, and how to meet your accountability obligations. It does not impose any additional barriers to data sharing, but will help you comply with your legal obligations under the UK GDPR and the DPA 2018.

It also contains some optional good practice recommendations, which do not have the status of legal requirements but aim to help you adopt an effective approach to data protection compliance.

In accordance with section 127 of the DPA 2018, the Commissioner must take the code into account when considering whether you have complied with your data protection obligations when sharing data. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the UK GDPR or the DPA 2018 and in the use of her [enforcement powers](#).

The code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant.

## Further Reading

[↗ Relevant provisions in the legislation - see DPA 2018 sections 121](#) [↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 sections 125](#) [↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 sections 127](#) [↗](#)

External link

## How is the code affected by the UK's exit from the European Union?

Now the UK has left the EU, a UK version of the EU GDPR has been written into UK law as the UK GDPR to sit alongside the DPA 2018.

The EU GDPR may still apply to you if you operate in the European Economic Area (EEA) or offer goods and services to individuals or monitor the behaviour of individuals there. Rules on international transfers now apply to the flow of data to and from the EEA.

If there are any further changes to the details of the future UK regime, the Commissioner will publicise them, and will note the changes on the ICO website.

For the latest information and guidance on data protection and the UK's position regarding the EU, see the ICO website.

## Further Reading

[↗ Relevant provisions in the legislation - see DPA 2018 section 207](#) [↗](#)

External link

### Further reading

[International transfers](#)

[Data protection at the end of the transition period](#)

UK Government website: [Brexit: new rules are here](#) [↗](#)

## What happens if we don't comply with the code?

If you don't comply with the guidance in this code, you may find it more difficult to demonstrate that your data sharing is fair, lawful and accountable and complies with the UK GDPR or the DPA 2018.

If you process personal data in breach of this code and this results in a breach of the UK GDPR or the DPA 2018, we can take action against you.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, we have the power to issue fines of up to £17.5 million or 4% of your annual worldwide turnover, whichever is higher.

There is no penalty if you fail to adopt good practice recommendations, as long as you find another way to comply with the law.

For more information, see the section on [enforcement of this code](#).

## What is the purpose of this code?

It provides practical guidance for organisations about sharing personal data in a way that complies with data protection law. It explains the law and promotes good practice. It dispels myths and misconceptions about data sharing.

Many organisations using this code of practice will have already shared data under the former data protection regime. The code should give you the knowledge and the confidence you need to continue sharing data under the UK GDPR and the DPA 2018 and assess how to share personal data in new projects and programmes. You should use the code to help you review and, where necessary, update ongoing data sharing arrangements.

The code of practice:

- updates and reflects key changes in data protection law since the last data sharing code was published (in particular from the UK GDPR and the DPA 2018);
- explains new developments and their impact on data protection;
- references new areas for you to consider; and
- helps you to manage risks in sharing data, which are magnified if the quantity of data is large.

## Who is this code for?

The code is mainly aimed at organisations that are controllers sharing personal data. In particular, it is aimed at data protection officers (DPOs) and other individuals within organisations who are responsible for data sharing matters.

Please see the sections below on joint controllers and processors.

In the code the reader is addressed by the term 'you' (and by the term 'we' in some headings that take the form of questions). It uses this terminology to refer to organisations that are sharing data or considering doing so. The code will also be helpful to controller organisations receiving shared data.

Controllers are defined under Article 4 of the UK GDPR and section 32 of the DPA 2018 as having responsibility for deciding the "purposes and means of the processing of personal data".

The code is also aimed at controllers sharing data under the law enforcement processing regime (Part 3 DPA 2018), and between the UK GDPR/Part 2 DPA 2018 and Part 3 DPA 2018. There is a [separate section about this](#), but the code includes references to some Part 3 provisions throughout to highlight significant differences. If you are one of these controllers, you should still read the whole of this code, which distinguishes between the regimes where appropriate.

Much of the advice is applicable to public, private and social sector organisations. Some of the code is necessarily focused on sector-specific issues. However, the majority of the code applies to all data sharing, regardless of its scale and context.

Reading and understanding this code and adopting its practical recommendations will give you confidence to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

The code will help you identify what you need to consider before you share personal data and clarify when it is appropriate for you to do so.

## Common misconceptions about data sharing

The code also clears up misconceptions about data sharing and barriers to sharing.

It is true that data sharing can sometimes be a complex activity. But for some organisations the perceived risks of getting it wrong - in the shape of reputational damage or enforcement action by the regulator - outweigh the benefits that can be gained from data sharing, leading to missed opportunities for innovation and improved public services.

However, data protection law is an enabler for fair and proportionate data sharing, rather than a blocker. It provides a framework to help you make decisions about sharing data.

Many of the requirements of data protection law simply place on a statutory footing the good practice that you will already have followed, or plan to follow.

The key question is often not whether you can share data, but how.

For example:

### **Misconception**

The UK GDPR and the DPA 2018 prevent us from sharing data.

### **Reality**

This is mistaken. Data protection law does not prevent data sharing, as long as you approach it in a fair and proportionate way. If you were able to share data lawfully under the former data protection regime, it is likely that you are able to continue to do so now. While there are some differences, the new legislation helps you to ensure you are sharing data in a way that promotes trust and transparency.

### **Misconception**

There is little benefit to be gained from data sharing.

### **Reality**

Data sharing brings significant benefits to your organisation, to individuals and to society at large. Done well, it helps government, public, social sector and commercial organisations to deliver modern, more efficient services which better meet people's needs and make their lives easier. It can also identify people at risk, help protect them from harm and address problems before they have a significant adverse impact.

### **Misconception**

We can only share data with people's consent.

### **Reality**

Most data sharing does not rely on consent as the lawful basis.

If you cannot offer a genuine choice, consent is not appropriate. Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

### **Misconception**

We can't share data in an emergency.

### **Reality**

You can share data in an emergency; you should do whatever is necessary and proportionate.

Examples of an emergency situation are the risk of serious harm to human life, the protection of public health, or the protection of national security. Please see our section on this topic later in the code.

Where possible you should plan ahead and put contingencies in place.

## **The benefits of data sharing**

The code highlights the benefits that sharing personal data can bring to everyone: society, organisations, and individuals, whether as citizens or consumers.

Data sharing can help public bodies and other organisations to fulfil their functions and deliver modern, efficient services that make everyone's lives easier. It can help keep the vulnerable safe at times of crisis, and help to produce official statistics, research and analysis for better decision-making for the public good.

Conversely, not sharing data can mean that everyone fails to benefit from these opportunities; and in some instances the chance is missed to assist people in need, whether in urgent or longer-term situations.

### **Example**

In the banking sector, Open Banking enables businesses to offer services to customers using their personal data.

For example, a fintech company can offer a service helping a customer to save, by automatically transferring money from their account to savings every month based on an analysis of their

spending.

This use of their personal data benefits the customer by increasing their savings and reducing inconvenience for them. This all takes place within a framework that protects the customer's privacy.

It benefits the bank because it allows it to benchmark products against competitors and reach new customers more easily, and provides evidence for anti-fraud prevention checks and customer verification, which is also in the public interest.

### **Example**

A local area set up an integrated care record to share patient records between health and social care staff. This sharing between public and social sectors resulted in:

- a more holistic picture about a patient's health;
- coordinated and safer care across the region;
- better decision-making around a patient's care; and
- patients only having to tell their story once.

### **Example**

A private day nursery collected information about the behaviour of an adult towards a child in its care and found a concerning pattern.

The nursery shared this information with local authority safeguarding leads to protect the child and others, and to investigate the adult's behaviour.

### **Example**

Several health professionals from different organisations and care businesses were involved in providing health and social care to a group of older adults. By exchanging information about recent changes in behaviour from one of the clients, they identified a pattern of evidence indicating the person might be a victim of abuse. To ensure the safeguarding of the person, they shared this information with the person's social worker for further investigation.

## How should we use this code?

The code covers data sharing by controller organisations (organisations that determine how personal data is used) under two separate regimes:

- general processing under the UK GDPR, which has to be read together with Part 2 of the DPA 2018; and
- law enforcement processing under the law enforcement provisions in Part 3 of the DPA 2018.

It also covers data sharing between the two regimes.

Most data sharing is likely to be under the UK GDPR and Part 2 of the DPA 2018 because it involves sharing data that is not law enforcement or intelligence personal data, but where provisions differ we clarify this as far as possible. The main body of the code therefore applies to processing under the UK GDPR and Part 2 of the DPA 2018. There is a [separate section in this code on law enforcement processing under Part 3 of the DPA 2018](#) that describes the differences in more detail, but controllers carrying out that type of processing should still read the whole of the code.

While the code does not cover the details of data sharing under the intelligence services regime in Part 4 of the DPA 2018, it is relevant to that regime, subject to the specific provisions of Part 4.

The code also discusses data sharing for defined purposes across the public sector under the Digital Economy Act 2017.

The code is complementary to other ICO guidance and codes of practice about data protection. It assumes knowledge of key data protection terms and concepts. While the code stands as your guide to data sharing, it does not seek to reproduce other ICO guidance, and you might need at times to refer to guidance on the ICO website or contact our helpline. The code will highlight particular instances when it would be useful for you to refer to such guidance.

In particular, you will find it helpful to use the data protection impact assessment (DPIA) process along with the code when considering sharing data. Some or all of the DPIA questions are likely to help you when you are assessing whether it is appropriate to share data, and whether it would be in compliance with the law. You can find more on DPIAs later in the code.

Another area where you will find it helpful to refer to detailed ICO guidance is in checking whether an exception, exemption or restriction applies in your circumstances, under the UK GDPR or the DPA 2018.

For instance, if an exemption applies under the DPA 2018, you may not have to comply with all the usual rights and obligations. There is a wide range of exemptions relating to matters such as crime and taxation, certain regulatory functions, journalism, research and statistics, and archiving in the public interest.

### Using the code

The code is divided into sections headed by each topic, and there are links to content in the guide to Navigating the data sharing code, and throughout the code to help you find your way around it.

As stated above, you will find it helpful to refer to other information and guidance. Because the code is statutory and is not readily updatable, any hyperlinks to guidance, tools and further information from the ICO or other sources are contained in boxes headed "Further reading". These links do not form part of the code.

To clarify any unfamiliar terms and acronyms, you may also wish to refer to the Glossary towards the end of the code.



We have used examples in the code to illustrate the law and good practice. You can find longer case studies in Annex C.

In addition to linking to sources of information outside the code (for example, links to guidance, such as on conducting a DPIA) the code contains tools for you to use:

- The guide to Navigating the data sharing code directs you to the section of the code that you need.
- Annex A is a checklist to help you decide whether or not to share data.
- Annex B contains template data sharing request and decision forms.

### Further reading

[Guide to data protection](#)

[Guide to Law Enforcement Processing](#)

[Guidance on exemptions](#)

Further resources and support are available on the ICO [data sharing information hub](#).

## Why should we use the data sharing code?

The benefits for you in adopting the recommendations in the code may include:

- greater trust in you by the public and customers, whose data you may want to share;
- an improved understanding of whether and when it is appropriate to share personal data;
- greater confidence within your organisation that you are sharing data appropriately and correctly;
- the confidence to share data in a one-off situation or in an emergency;
- a reduced reputational risk when sharing data;
- more robust, demonstrable compliance with the law; and
- better protection for individuals whose data you are sharing.

## Further Reading

 [Relevant provisions in the legislation - see UK GDPR Articles 4\(7\) and 4\(8\)](#) 

External link

 [Relevant provisions in the legislation - see DPA 2018 section 3\(9\)](#) 

External link

 [Data sharing hub](#)

For organisations

### Further reading

[Controllers and processors](#)



# Data sharing covered by the code

## At a glance

The code covers the sharing of personal data between organisations that are controllers.

It includes when you give access to data to a third party, by whatever means.

Data sharing can take place in a routine, scheduled way or on a one-off basis.

When needed, you can share data in an urgent or emergency situation.

## In more detail

- [Data sharing between controllers](#)
- [Sharing data with a processor is not covered by the code](#)
- [“Data sharing” within an organisation is not covered by the code](#)
- [Data sharing covered by the code](#)
- [Routine data sharing](#)
- [Ad hoc or one-off data sharing](#)
- [Data pooling](#)

### Data sharing between controllers

The code focuses on the sharing of personal data between controllers, ie where separate or joint controllers determine the purposes and means of the processing of personal data, as defined in UK GDPR Article 4(7).

### Sharing data with a processor is not covered by the code

If a controller asks another party to process personal data on its behalf, for the purposes of the UK GDPR the other party is a “processor”, as defined in Article 4(8) of the UK GDPR. The UK GDPR draws a distinction between a controller sharing personal data with another controller, and a processor processing personal data on behalf of a controller.

Article 28 of the UK GDPR lays down requirements that must be in place between a controller and processor, in order to protect the rights of the data subject. These requirements include a written contract and guarantees about security. Under the UK GDPR a processor must only process personal data on documented instructions from the controller. A processor has its own liabilities and responsibilities both under the contract and the UK GDPR.

This type of processing arrangement is outside the scope of this code, but further information is available on the ICO website.

### “Data sharing” within an organisation is not covered by the code

The code does not apply to the disclosure of data within the same organisation, where the controller is one

---

and the same. The movement of data by one part of an organisation to another part - by the controller to itself - is not data sharing. The other obligations under data protection law obviously still apply, however.

## Data sharing covered by the code

There is no formal definition of data sharing within the legislation, although the scope of this code is defined by section 121 of the DPA 2018 as “the disclosure of personal data by transmission, dissemination or otherwise making it available”. This includes:

- providing personal data to a third party, by whatever means;
- receiving personal data as a joint participant in a data sharing arrangement;
- the two-way transmission of personal data; and
- providing a third party with access to personal data on or via your IT systems.

For the purposes of this code, data sharing does not include providing data access to employees or contractors, or with processors such as third-party IT processors. Please read the paragraphs later in this section on sharing data with processors.

The following examples illustrate a range of data sharing types within the scope of the code:

- a one-way or reciprocal exchange of data between organisations;
- an organisation providing another organisation with access to personal data on its IT system for a specific research purpose;
- several organisations pooling information and making it available to each other or to a third party or parties;
- data sharing on a routine, systematic basis for an established purpose;
- one-off, exceptional or ad hoc data sharing; and
- one-off data sharing in an urgent or emergency situation.

### **Examples of real-life data sharing activities**

- a bank disclosed personal data about its employees to an anti-fraud body;
- a primary school passed details about a child showing signs of harm to the police and social services;
- the police and Border Force exchanged information about individuals thought to be involved in serious crime;
- a supermarket gave information about a customer’s purchases to the police following an allegation of shoplifting;
- a secondary school provided information about its pupils to a research company for research purposes; and
- a multi-agency network group regularly exchanged information about individuals for safeguarding or social care purposes.

The code only applies to sharing personal data. Neither the UK GDPR, the DPA 2018, nor this code, applies

to sharing information that does not constitute personal data. Some sharing doesn't involve personal data; for example, if an organisation is sharing information that cannot identify anyone (anonymous information; please refer to the ICO website for forthcoming guidance on anonymisation).

### **Example**

These are two examples of data sharing, one of which is subject to the UK GDPR and the second which is not.

A travel business collects data on individual travel movements. Prior to sharing with third parties, it removes directly identifiable information such as name or address from the data. In this case, it is still personal data as it is very likely that an individual could be identified by combining the data with other available information; for example, social media accounts. This will be considered personal data under the UK GDPR.

However, if the travel business shares high-level aggregate statistics with third parties, for example: "on Fridays, for a particular journey there are 130% fewer passengers than on Tuesdays", no individual can be identified. Therefore this would qualify as anonymous information and is not personal data under the UK GDPR.

The position is different for pseudonymised data. Data which has undergone pseudonymisation is defined in the UK GDPR as data that can no longer be attributed to a data subject without the use of additional information. If you have pseudonymised the data according to the definition of the UK GDPR, such that the additional information could be used to re-identify a data subject within that data, then you must treat the pseudonymised data as personal data.

It is common to consider data sharing as falling into two main types of scenario:

- data sharing on a frequent and/or regular basis, also known as routine or 'systematic' data sharing, where the same data sets are regularly shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for a purpose that is ad hoc, unexpected or due to an urgent situation or an emergency.

Different approaches apply to these two scenarios, and the code reflects this. Most of the code concentrates on routine data sharing.

### **Routine data sharing**

This is data sharing done on a regular basis in a routine, pre-planned way. It generally involves sharing data between organisations for an established purpose - perhaps with standardised data structures and values - at regular, scheduled intervals.

For example, a group of organisations might make an arrangement to share or pool their data for specific purposes, again on a frequent and/or regular basis.

If you are carrying out this type of data sharing, you should establish rules and agree procedures in advance.

## Ad hoc or one-off data sharing

It is good practice to formalise your data sharing through a data sharing agreement. However in some instances you may decide, or be asked, to share data in ad hoc situations that are not covered by any routine arrangement or agreement. It is still possible to share data in this situation, but you should carefully assess the risks every time. We recommend that you make plans to cover such contingencies.

Sometimes you may have to make a decision quickly about data sharing in conditions of real urgency, or even in an emergency situation. You should not be put off from data sharing in a scenario like this; in an urgent situation you should assess the risk and do what is necessary and proportionate. Please see the section later in this code on [Data sharing in an urgent situation or in an emergency](#).

## Data pooling

Data pooling is a form of data sharing where organisations decide together to pool information they hold and make it available to each other, or to different organisations, for a specific purpose or purposes. The organisations should consider whether they are separate or joint controllers.

If the organisations are joint controllers, under Article 26 of the UK GDPR they must enter into a formal, transparent arrangement setting out agreed roles and responsibilities for complying with the UK GDPR. For more details, you should refer to the guidance on controllers and processors on the ICO website.

### Further reading


[Contracts and liabilities between controllers and processors](#)

[Key definitions: controllers and processors](#)

[Controllers and processors](#)

[What does it mean if you are joint controllers?](#)

## Further Reading

[Relevant provisions in the legislation - see UK GDPR Articles 4, 26, 28, 82 and 83](#) 

External link

[Relevant provisions in the legislation - see UK GDPR Recitals 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 79, 81, 82 and 146](#) 

External link

[Relevant provisions in the legislation - see DPA 2018 section 121](#) 

External link

# Deciding to share data

## At a glance

In addition to considering whether the data sharing achieves a benefit and is necessary, you must consider your overall compliance with data protection law when sharing data.

We recommend that as a first step you carry out a Data Protection Impact Assessment (DPIA), even if you are not legally obliged to carry one out. Carrying out a DPIA is an example of best practice, allowing you to build in openness and transparency.

A DPIA will help you assess the risks in your planned data sharing and determine whether you need to introduce any safeguards. It will help you assess those considerations, and document them. This will also help to provide reassurance to those whose data you plan to share.

## In more detail

- [What do we need to consider?](#)
- [Do we need to do a DPIA?](#)

### What do we need to consider?

We have described earlier the benefits of data sharing to society, to organisations, and to us all as citizens and consumers.

When thinking about sharing data, as well as considering whether there is a benefit to the data sharing and whether it is necessary, you must consider your overall compliance with data protection legislation, including fairness and transparency.

As a first step, we recommend that you carry out a Data Protection Impact Assessment (DPIA). A DPIA is an invaluable tool to help you assess any risks in your proposed data sharing, and work out how to mitigate these risks. It will help you to ensure you are sharing data fairly and transparently. It will help you to consider these matters, and to document them.

In law you are required to consider doing a DPIA. However, even if you are not legally obliged to carry one out, it is very beneficial for you to follow the DPIA process.

### Do we need to do a DPIA?

We recommend that you carry out a DPIA, as it can benefit both you and the public whose data you plan to share. It will help you to:

- assess any risks in your planned data sharing; and
- promote public trust in your data sharing plans.

You are obliged to carry out a DPIA for data sharing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.

To help you determine whether you need to carry out a DPIA, you can:

- use our screening checklists on the ICO website; and
- read the detailed guidance on DPIAs on the ICO website.

It is good practice to carry out a DPIA if you have a major project that involves disclosing personal data, or any plans for routine data sharing, even if there is no specific indicator of likely high risk.

If you have taken into account the nature, scope, context and purposes of the sharing and you are confident that the type of data sharing you have in mind is unlikely to result in high risk, you are not legally required to carry out a DPIA.

However, we recommend that you carry out a DPIA even where you are not legally obliged to do so. You can use the DPIA process as a flexible and scalable tool to suit your project. A DPIA is a practical tool that will help you assess the risks in any planned data sharing. A DPIA need not be a 'bolt-on' process - you can integrate the DPIA into any risk frameworks your organisation may already have in place.

As already stated in this code, data sharing must be done in a fair and proportionate way. Using the DPIA to assess the risks in your proposed data sharing will help you achieve that proportionality, as the process will help you to fully understand:

- whether you can share the data at all; and
- whether you can share the data, but with steps to mitigate the risks.

Therefore, the DPIA process will help not only to ensure the protection of the data, but will also help you to put additional safeguards in place to mitigate risk where needed. In turn, this will help to provide reassurance to the people whose data you are sharing.

## Further Reading

[↗ Relevant provisions in the legislation - see UK GDPR Articles 35 and 36 ↗](#)

External link

[↗ Relevant provisions in the legislation - see UK GDPR Recitals 74-77, 84, 89-92, 94 and 95 ↗](#)

External link

### Further reading

[Data protection impact assessments](#)

[Detailed guidance on DPIAs](#)

[DPIA sample template](#)

[DPIA checklists](#)

The former Article 29 Working Party (WP29) produced [guidelines on data protection impact assessments](#) ↗, which have been endorsed by the European Data Protection Board (EDPB). The EDPB, which replaced WP29, includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU GDPR. Whilst EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime, they may still provide helpful guidance on certain issues.





# Data sharing agreements

## At a glance

It is good practice to have a data sharing agreement.

Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities.

Having a data sharing agreement in place helps you to demonstrate you are meeting your accountability obligations under the UK GDPR.

## In more detail

- [Introduction](#)
- [What are the benefits of a data sharing agreement?](#)
- [What should we include in a data sharing agreement?](#)
- [When should we review a data sharing arrangement?](#)

## Introduction

A data sharing agreement between the parties sending and receiving data can form a major part of your compliance with the accountability principle, although it is not mandatory. Your organisation might use a different title for a data sharing agreement, for example:

- an information sharing agreement;
- a data or information sharing protocol or contract; or
- a personal information sharing agreement.

Whatever the terminology, it is good practice to have a data sharing agreement in place.

Government departments and certain other public bodies (for example, regulators, law enforcement bodies and executive agencies) may enter into a memorandum of understanding with each other that includes data sharing provisions and fulfils the role of a data sharing agreement.

However on their own, the following do not constitute a data sharing agreement:

- a memorandum of understanding (except between government departments and certain other public bodies);
- a list of standards; or
- an addendum to a purchase agreement or to a purchase order or proposal.

## What are the benefits of a data sharing agreement?

A data sharing agreement:

- helps all the parties be clear about their roles;
- sets out the purpose of the data sharing;
- covers what happens to the data at each stage; and
- sets standards.

It should help you to justify your data sharing and demonstrate that you have been mindful of, and have documented, the relevant compliance issues. A data sharing agreement provides a framework to help you meet the requirements of the data protection principles.

There is no set format for a data sharing agreement; it can take a variety of forms, depending on the scale and complexity of the data sharing. Since a data sharing agreement is a set of common rules that binds all the organisations involved, you should draft it in clear, concise language that is easy to understand.

Drafting and adhering to a data sharing agreement should help you to comply with the law, but it does not provide immunity from breaching the law or from the consequences of doing so. However, the ICO will take into account the existence of any relevant data sharing agreement when assessing any complaint we receive about your data sharing.

## What should we include in a data sharing agreement?

You should address a range of questions in a data sharing agreement.

### **Who are the parties to the agreement?**

Your agreement should state who the controllers are at every stage, including after the sharing has taken place.

### **What is the purpose of the data sharing initiative?**

Your agreement should explain:

- the specific aims you have;
- why the data sharing is necessary to achieve those aims; and
- the benefits you hope to bring to individuals or to society more widely.

You should document this in precise terms so that all parties are absolutely clear about the purposes for which they may share or use the data.

### **Which other organisations will be involved in the data sharing?**

Your agreement should clearly identify all the organisations that will be involved in the data sharing and should include contact details for their data protection officer (DPO) or another relevant employee who has responsibility for data sharing, and preferably for other key members of staff. It should also contain procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing.

### **Are we sharing data along with another controller?**

If you are acting with another controller as joint controllers of personal data, there is a legal obligation to set out your responsibilities in a joint control arrangement, under both the UK GDPR/Part 2 of the DPA 2018 and under Part 3 of the DPA 2018. Although the code mainly focuses on data sharing between separate controllers, the provisions of a data sharing agreement could help you to put a joint control arrangement in

place.

### **What data items are we going to share?**

Your agreement should set out the types of data you are intending to share. This is sometimes known as a data specification. This may need to be detailed, because in some cases it will be appropriate to share only certain information held in a file about an individual, omitting other, more sensitive, material. In some cases it may be appropriate to attach 'permissions' to certain data items, so that only particular members of staff or staff in specific roles are allowed to access them; for example, staff who have received appropriate training.

### **What is our lawful basis for sharing?**

You need to clearly explain your lawful basis for sharing data. The lawful basis for one organisation in a data sharing arrangement might not be the same as that for the other one.

If you are using consent as a lawful basis for disclosure, then your agreement should provide a model consent form. You should also address issues surrounding the withholding or retraction of consent.

You should also set out the legal power under which you are allowed to share the data.

### **Is there any special category data, sensitive data or criminal offence data?**

You must document the relevant conditions for processing, as appropriate under the UK GDPR or the DPA 2018, if the data you are sharing contains special category data or criminal offence data under the UK GDPR, or there is sensitive processing within the meaning of Part 3 of the DPA 2018.

### **What about access and individual rights?**

You should set out procedures for compliance with individual rights. This includes the right of access to information as well as the right to object and requests for rectification and erasure. You must make it clear in the agreement that all controllers remain responsible for compliance, even if you have processes setting out who should carry out particular tasks.

For example, the agreement should explain what to do when an organisation receives a request for access to shared data or other information, whether it is under the data protection legislation, or under freedom of information legislation. In particular, given data subjects can contact any controller involved in the sharing, it should make clear that one staff member (generally a DPO in the case of personal data) or organisation takes overall responsibility for ensuring that the individual can easily gain access to all their personal data that has been shared.

For joint controllers, Article 26 of the UK GDPR and section 58 of the DPA 2018 for Part 3 processing require you to state in the agreement which controller is the contact point for data subjects.

You will have to take decisions about access on a case-by-case basis.

For public authorities, the agreement should also cover the need to include certain types of information in your freedom of information publication scheme.

There are more details on individual rights under the UK GDPR/Part 2 of the DPA 2018 and under Part 3 of the DPA 2018 in the section of this code on the rights of individuals. There is also more information on Part 3 in the section in this code on law enforcement processing.

### **What information governance arrangements should we have?**

Your agreement should also deal with the main practical problems that may arise when sharing personal data. This should ensure that all organisations involved in the sharing:

- have detailed advice about which datasets they can share, to prevent irrelevant or excessive information being disclosed;
- make sure that the data they are sharing is accurate, for example by requiring a periodic sampling exercise and data quality analysis;
- record data in the same format, abiding by open standards when applicable. The agreement could include examples showing how to record or convert particular data items, for example dates of birth;
- have common rules for the retention and deletion of shared data items, as appropriate to their nature and content, and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;
- have common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement in a timely manner;
- ensure their staff are properly trained and are aware of their responsibilities for any shared data they have access to;
- have procedures for dealing with access requests, complaints or queries from members of the public;
- have a timescale for assessing the ongoing effectiveness of the data sharing initiative and the agreement that governs it; and
- have procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

### **What further details should we include?**

It is likely to be helpful for your agreement to have an appendix or annex, including:

- a summary of the key legislative and other legal provisions, for example relevant sections of the DPA 2018, any law which provides your legal power for data sharing and links to any authoritative professional guidance;
- a model form for seeking individuals' consent for data sharing, where that is the lawful basis; and
- a diagram to show how to decide whether to share data.

You may also want to consider including:

- a data sharing request form; and
- a data sharing decision form.

You can find examples of these in the Annex to this code.

### **When should we review a data sharing arrangement?**

You should review your data sharing arrangements on a regular basis; and particularly when a change in circumstances or in the rationale for the data sharing arises. You should update your data sharing agreement to reflect any changes. If there is a significant complaint, or a security breach, this should be a trigger for you to review the arrangement.

# Data protection principles

When sharing data, you must follow the data protection principles.

As previously stated, a data sharing agreement will provide a framework to help you to do this.

There are some differences between the principles in the respective pieces of legislation:

- the UK GDPR and Part 2 of the DPA 2018 for general data processing; and
- Part 3 of the DPA 2018 for law enforcement processing.

You should refer to the detailed guidance on the ICO website.

## Further Reading

[Relevant provisions in the legislation - see UK GDPR Article 5](#)

External link

[Relevant provisions in the legislation - see UK GDPR Recital 39](#)

External link

[Relevant provisions in the legislation - for Law Enforcement Processing under Part 3 of the DPA 2018, see sections 34-40](#)

External link

### Further reading

[The principles](#)

[Guide to Law Enforcement Processing](#)

# Accountability

## At a glance

Accountability should form an important part of the culture and business of your organisation.

The specific accountability requirements of the UK GDPR mean that you are responsible for your compliance with the UK GDPR or the DPA 2018. You must be able to demonstrate that compliance.

You should review all your accountability measures regularly.

## In more detail

- [What is accountability?](#)
- [What documentation do we need to keep?](#)
- [What is the role of the data protection officer \(DPO\) in a data sharing arrangement?](#)

## What is accountability?

Accountability is a legal requirement for data sharing; it is one of the principles applicable to general data processing under the UK GDPR. The importance of accountability cannot be overstated. To be effective, you have to embed the message of accountability in the culture and business of your organisation, from board level through to all your employees and contractors.

You must consider the risks data sharing may create, and take appropriate action. You need to ensure staff are adequately trained, assess your data processing and put data protection at the heart of your organisation. It is more than box ticking or bolt-on compliance. It is an opportunity to make data protection a part of the cultural and business fabric of your organisation. It means not only complying with the legislation, but showing it.

Accountability obligations mean that if you are involved in a data sharing arrangement, you are responsible for your compliance with the UK GDPR or DPA 2018, and you must be able to demonstrate that compliance. As part of this, and where proportionate, you must put in place a data protection policy which adopts a "data protection by design and default" approach. This will help you comply with data protection law and good practice whenever you process data.

There is a general obligation to evidence your compliance and justify your approach, so you should maintain relevant documentation and adopt additional measures as necessary. A data sharing agreement is one example of good practice to demonstrate you are meeting your accountability obligations. If you are unable to justify your approach, it is likely you will fail to meet those obligations.

Successfully embedding accountability will enhance your reputation as a business that can be trusted with personal data. The public are increasingly demanding to be shown how their data is being used and how it is being looked after. They want to know that their personal data is in safe hands, and that you have put in place mechanisms to protect their information.

For law enforcement processing, similar provisions are set out in Chapter 2 of Part 3 of the DPA 2018.

## What documentation do we need to keep?

Accountability should form part of a long-term programme of compliance and sound governance within your organisation. Documentation forms one of the requirements to ensure effective accountability, and the UK GDPR is specific on this point. Under Article 30 of the UK GDPR, larger organisations are required to maintain a record of their processing activities. Even if you are not a larger organisation, you should document any data sharing you undertake, and review it regularly.

Documenting this information is a practical way of taking stock of your data sharing. Knowing what information you have, where it is, and what you do with it makes it much easier for you to comply with other aspects of the UK GDPR, such as making sure that you hold accurate and secure information. You should follow good records management practice, and for this purpose you may find it helpful to refer to the codes of practice under section 46 of the Freedom of Information Act 2000 (FOIA) and section 61 of the Freedom of Information (Scotland) Act 2002 (FOISA).

As well as any record of all aspects of the data sharing and other processing activities required under Article 30, you must keep sufficient documentation to demonstrate your compliance with the UK GDPR when sharing data, such as:

- your compliance with all data protection principles, obligations and rights;
- your record of the lawful basis for processing and the privacy information you provide;
- any records of consent; and
- records of any personal data breaches.

For data sharing that constitutes law enforcement processing under Part 3 of the DPA 2018, section 61 of the DPA 2018 sets out the records to keep, including logs of processing operations in automated processing systems.

## What is the role of the data protection officer (DPO) in a data sharing arrangement?

If you have a DPO, they should be closely involved from the outset in any plans to enter into a data sharing arrangement. Some organisations may have multiple individuals with responsibility for data sharing matters, depending on the context of the data sharing and the arrangements within the organisation. Many of the references to the DPO in this code are applicable to them as well. In all cases, you should document the advice you receive from them.

DPOs play an important role while a data sharing arrangement is under way. Since there will be a number of organisations involved, each of you will have your own responsibilities for the data you share or have received. Often a data sharing arrangement involves processing sensitive information. In each of the organisations, the DPO advises everyone on information governance, ensures compliance with the law, and provides advice to staff faced with decisions about data sharing. They may also be a contact point for individuals to exercise their rights.

The ICO's main contact point with an organisation is through the DPO and we are here to advise and address their concerns.

### **Example**

An airline looked to develop its service by improving transport schedules, mitigating disruption for passengers and taking steps to improve its carbon footprint. To do this, the airline wanted to use



the personal data that it held about its customers for a new purpose.

It considered the requirements of Article 6.4 of the UK GDPR and undertook a DPIA, as the processing required the combination of different datasets.

To implement some of the strategies proposed, the airline needed to provide some of the data to a partner company which had developed software to enhance customer engagement in this area. In sharing the data, the airline considered whether the partner company adhered to appropriate security measures and had a written contract covering the scope of the data sharing and processing.

In this case, the airline had implemented a 'data protection by design and default' approach. It had:

- taken appropriate measures to establish if the new processing arrangements were lawful
- been clear with the third party about the extent of the processing permitted; and
- had kept clear evidence of the steps taken to comply with the requirements of the UK GDPR.

### **Example**

A police intelligence database on gangs in an area (the gangs database) had been shared by the police with the local authority. The council went on to share it inappropriately with a number of organisations. This constituted a data breach.

Shortly afterwards there were incidents of gang violence in the area and some victims had featured in the gangs database. Although it was not possible to establish a causal connection to the data breach, it was obvious that there was a risk of distress and harm when this type of sensitive data was not kept secure.

In this case, it was apparent that it was unfair and excessive for the council to have shared the unredacted database with a large number of people and other organisations. It should have realised that there was an obvious risk in doing so.

There is a national concern about the need to tackle gang crime, and it is widely recognised that this is a challenge for public authorities. Data sharing has an important role to play in tackling this challenge; however, it has to be carried out in compliance with the law. Data must be processed lawfully, fairly, proportionately and securely. However, data protection law is not a barrier to data sharing.

To help prevent such incidents happening, organisations processing sensitive data should have in place policies, processes and governance, as well as training for staff. Conducting a DPIA is one way an organisation can try to ensure it is complying with the law. This data sharing code also provides practical information.

## Example

A health care organisation provided an out-of-hours emergency telephone service. As calls could be received about clients' welfare, it was essential that advisors had access to some personal data about the organisation's clients to carry out their role and where appropriate to share data in the public interest.

A call was taken by a new advisor late one evening from someone identifying themselves as a police officer and requesting the address of one of the organisation's clients.

The organisation had protocols to follow about sharing data to third parties, and it was mandatory that all new advisors had this training on appointment. The advisor therefore knew the procedure to follow to determine whether or not they could share this information.

## Further Reading

[↗ Relevant provisions in the legislation - see UK GDPR Articles 5.1\(b\), 5.2, 6.4, 25, 28,29,30,31,32,34,35, 38, 39 ↗](#)

External link

[↗ Relevant provisions in the legislation - see UK GDPR Recitals 39, 81-83 ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 Part 3, Sections 61 and 62 ↗](#)

External link

## Further reading

[Guidance on DPIAs, DPOs, documentation and accountability ↗](#)

[ICO's Accountability Framework ↗](#)

[Data protection by design and default](#)

[Guide to Law Enforcement Processing](#)

[Sharing personal data with law enforcement authorities](#)

[Data sharing and re-use of data by competent authorities for non-law enforcement purposes](#)

[The Lord Chancellor's code of practice on records management under section 46 FOIA](#)

[Scottish government code of practice on records management under section 61 FOISA](#)

[What happens if we have a new purpose?](#)

[Purpose limitation](#)

# Fairness and transparency in data sharing

## At a glance

The gateway to getting data sharing right is always to share personal data fairly and in a transparent manner.

- You must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them.
- When you share personal data, you must ensure it is reasonable and proportionate.
- You must ensure that individuals know what is happening to their data.
- Before sharing data, you must tell individuals about what you propose to do with their personal data in a way that is accessible and easy to understand.

Fairness and transparency are fundamental to your approach to sharing data under the UK GDPR, and they are closely linked. Understanding that you are responsible for ensuring fairness and transparency will help you to ensure your general compliance with data protection law.

Fairness also forms a key part of the principles under the law enforcement provisions of Part 3 of the DPA 2018. However, the principles in Part 3 do not include transparency; this is due to the potential to prejudice an ongoing law enforcement investigation in certain circumstances. It is essential that the law enforcement agencies have the powers that they need to investigate crimes and bring offenders to justice. However, section 44 of the DPA 2018 sets out the information a controller should make available to data subjects for law enforcement processing purposes.

As part of fairness and transparency considerations, you should also bear in mind ethical factors when deciding whether to share personal data; ask yourself whether it is right to share it.

### Example

Two county councils and 19 relevant partner organisations (both public and private sector) decided to share personal information in order to prevent social exclusion amongst young people who had been, or were at high risk of, disengaging from education, employment or training. By sharing information, the partner organisations aimed to co-ordinate their approach to identifying and contacting each young person to support and encourage them back into education, or into work or training.

While the partner organisations took the view that the data sharing would benefit the young people, data protection law required them to consider whether it was fundamentally fair to the young people. The organisations had to pause and consider certain questions before deciding they could go ahead with the sharing:

- Would they only be sharing data in a way that would be in line with the reasonable expectations of the individuals concerned?
- How sure were they that they would not be sharing data in a way that would adversely affect the individuals?
- Did they mislead the individuals when they collected their personal data?

The organisations also had to consider whether they had met their transparency obligations:

- Were they open and honest with the individuals as to how they would use their personal data?
- Did they tell the individuals about the proposed use of their personal data in a clear, accessible way?

The councils were not prevented by data protection law from sharing data, but had to be sure they had done so fairly and transparently by answering these questions.

## Further Reading

[Relevant provisions in the legislation - see UK GDPR Articles 5.1\(a\), 13, 14](#) 

External link

[Relevant provisions in the legislation - see UK GDPR Recitals 39, 58, 60-62](#) 

External link

[Relevant provisions in the legislation - see DPA 2018 Part 3 section 44](#) 

External link

### Further reading

[Guidance on the right to be informed](#)

[Guidance on the first principle](#)

[Guide to Law Enforcement Processing: principles](#)

[Guidance on exemptions](#)

# Lawfulness

## At a glance

In order to comply with the lawfulness principle, you must ensure that your data sharing is lawful in a general sense.

This includes checking that you have a legal power to share data.

The legal power to share data is separate from the lawful basis provisions.

## In more detail

- [Introduction](#)
- [Do we have a legal power to share data?](#)
- [What are the legal powers in the public sector?](#)
- [What are the legal powers for private and social sector organisations?](#)
- [What is the impact of human rights law?](#)
- [Have we checked whether there are any additional legal requirements that need to be met when sharing data?](#)

## Introduction

This section looks at the principle of lawfulness and discusses the legal constraints on you, outside data protection legislation, and the legal powers you have to share data.

Before sharing any personal data, you must consider all the legal implications. You must ensure that your data sharing is lawful in a general sense in order to comply with the lawfulness principle. For public sector bodies, this includes identifying whether you have a legal power to share data.

Compliance with the lawfulness principle is in addition to identifying a lawful basis for your data sharing. Do not confuse lawful basis with general lawfulness or legal powers that are beyond the UK GDPR/DPA 2018. However, there is a link with the lawful bases - if you do not have a lawful basis to share data, you will be in breach of the lawfulness principle.

This might sound complex, so this section will break down the different elements you should consider.

## Do we have a legal power to share data?

If you wish to share personal data with another organisation, either by a one-off disclosure or as part of a routine data sharing arrangement, you need to consider:

- what type of organisation you are, because your legal status also affects your ability to share information. In particular, it depends on whether you are within the public, private or social sector; and
- whether you have a general legal power to share information, for instance, under the law setting you up, or under your constitution. This is likely to be more relevant to public sector organisations.

## What are the legal powers in the public sector?

Public sector organisations must check that they have the legal power to share data. When deciding whether you may proceed with any data sharing initiative, you should identify and document the law that is relevant to you. Even if this does not mention data sharing explicitly (and usually it doesn't) it is likely to lead you to a clearer understanding of your legal position.

Public sector organisations mostly derive their powers from sources such as the Act of Parliament or Royal Charter which set them up, or from case law, or duties under common law, or other laws regulating their activities. Government departments headed by a Minister of the Crown have common law powers to share information.

The relevant legislation probably defines your functions in terms of your purposes, the things that you must do and the powers you may exercise in order to achieve those purposes. So you should identify where the data sharing would fit, if at all, into the range of things that you are able to do. Broadly speaking, there are three ways in which you may do so:

- **Express statutory obligations**

Occasionally, a public body is legally obliged to share particular information with a named organisation. This is only the case in highly specific circumstances.

- **Express statutory powers**

Sometimes, a public body has an express power to share information. An express power is often designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways". For example, specific gateways exist under the Digital Economy Act 2017 (DEA). Under the DEA there is a framework providing a legal gateway for data sharing for defined purposes between specified public authorities, for the public benefit. There is a [separate section in this code on the DEA](#).

- **Implied statutory powers**

Often, the law regulating a public body's activities is silent on the issue of data sharing. In these circumstances, it may be possible to rely on an implied power to share information derived from the express provisions of legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted.

Public authorities are likely to rely on the public task lawful basis in Article 6.3 of the UK GDPR. This requires the legal power to be laid down by law; however it does not need to be contained in an explicit piece of legislation, but could be a common law task, function or power. You can rely on this power to share data so long as it is sufficiently foreseeable and transparent.

Whatever the source of your power to share information, you must check that the power covers that specific disclosure or data sharing arrangement. If it does not, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place.

## What are the legal powers for private and social sector organisations?

The legal framework that applies to private and social sector organisations differs from that for public

sector organisations. Most private and social sector organisations do not need to identify a specific power to share data. They have a general ability to share information, provided this does not breach the data protection legislation or any other law. If you are a private or social sector organisation you should check your constitutional documents, legal agreements or any other legal or regulatory requirements (such as the common law duty of confidentiality, or the Scottish law of privacy) to make sure you are complying with those requirements and that there are no restrictions that would prevent you from sharing personal data in a particular context. Big organisations with complex, larger scale processing should consider obtaining legal advice.

Private and social sector organisations should pay attention to any industry-specific regulation, guidance or UK GDPR code of conduct about handling personal data, as this might affect your ability to share information.

## What is the impact of human rights law?

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature.

Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights. Article 8 of the Convention, which gives everyone the right to respect for their private and family life, home and correspondence, is especially relevant to sharing personal data.

If you disclose or share personal data only in ways that comply with the data protection legislation, the sharing or disclosure of that information is also likely to comply with the HRA.

You should seek specialist advice if you have any concerns about human rights issues (other than the data protection elements of Article 8) regarding the disclosure or data sharing arrangement you are proposing.

## Have we checked whether there are any additional legal requirements that need to be met when sharing data?

Your ability to share information may be subject to a number of legal constraints outside data protection law. There might be other considerations such as specific legal requirements that need to be met, for example:

- prohibitions on sharing;
- copyright restrictions; or
- a duty of confidence that might affect your ability to share personal data.

A duty of confidence might be stated explicitly, or it might be implied, either by the content of the information or because it was collected in circumstances where confidentiality is expected (eg medical or banking information). If you are a big organisation planning to carry out complex, larger scale processing, you should consider obtaining legal advice on your data sharing plans.

In some private sector contexts, there are legal constraints on the disclosure of personal data, other than data protection law.

## Further Reading

---

### **Further reading**

[Lawfulness principle](#)

[Lawful basis for processing](#)

[Guide to Law Enforcement Processing](#)

[Sharing personal data with law enforcement authorities](#)

[Data sharing and re-use of data by competent authorities for non-law enforcement purposes](#)



# Lawful basis for sharing personal data

## At a glance

You must identify at least one lawful basis for sharing data before you start.

You must be able to show that you considered this before sharing any data, in order to satisfy the accountability principle.

## What are the provisions on lawful basis?

You must identify at least one lawful basis for sharing data. The lawful bases are different for:

- general processing under the UK GDPR and Part 2 of the DPA 2018; and
- law enforcement processing under Part 3 of the DPA 2018.

At least one lawful basis must apply before you start. You must be able to show that you considered this before sharing any data, in order to satisfy the accountability principle in the UK GDPR and in Part 3 of the DPA 2018. And without at least one lawful basis for processing, any data sharing you do will be in breach of the first principle in each piece of legislation.

### Example

A water company and an electricity network operator conducted a data sharing trial to share priority service data with one another. The two companies worked together to jointly identify and safeguard customers who might have found themselves in vulnerable circumstances if their services were disrupted.

Both companies previously held their own registers. The trial allowed the organisations to work together to simplify their processes and introduce a 'tell us once' style registration system. The organisations gained explicit consent from relevant customers before undertaking the trial, sharing the data manually and securely on Excel spreadsheets.

Due to the success of the trial, the two companies decided to continue the data sharing as part of their business as usual operations.

### Example

A government office responsible for overseeing business competition required information about the practices of a supermarket chain and its performance in the online retail sector.

To understand how the supermarket chain operated, the office gathered evidence about customers' online shopping habits. The data assisted the office in understanding the range and quality of online services provided by the supermarket chain, as well as its overall value.

As the review formed part of a statutory function, the office was able to demonstrate that the

processing was necessary in the public interest and relied on this as its lawful basis for obtaining the customer data from the supermarket chain.

### Example

A fintech company launched a paid-for digital tool to assist consumers in handling their finances. The tool could be viewed online and via a mobile phone application. It allowed individuals to access and consider their current accounts, savings accounts, credit cards, investments and pension information in one place. The tool also analysed spending habits and assisted the consumer in developing and managing their budgets. The analysis and planning could be addressed month by month and by different categories, such as grocery shopping, utilities and eating out.

For the service to function correctly, personal data needed to be shared with third-party providers. This was so the customer's experience could be personalised with third-party services and materials accessible via the tool.

The fintech company relied on 'performance of a contract' as its basis for processing under Article 6 of the UK GDPR. As some of the services required the provision of sensitive personal data, explicit consent was also relied on as a condition for processing under Article 9.

## Further Reading

[Relevant provisions in the legislation - see UK GDPR Articles 6.1\(c\), 6.1\(e\), 6.1\(f\), 6.3, 9.2, 13.1\(c\), 14.1\(c\)](#)

External link

[Relevant provisions in the legislation - see UK GDPR Recitals 39, 41, 45, 47-49, 50, 51](#)

External link

[Relevant provisions in the legislation - see DPA 2018 section 7](#)

External link

[Relevant provisions in the legislation - see DPA 2018 section 8](#)

External link

[Relevant provisions in the legislation - see DPA 2018 section 10](#)

External link

[Relevant provisions in the legislation - see DPA 2018 section 11](#)

External link

[Relevant provisions in the legislation - see DPA 2018 section 35](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 section 42 ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 Schedule 1 \(paras 6 and 7\) ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 Schedule 8 ↗](#)

External link

## Further reading

[Lawful basis for processing](#)

[Lawful basis interactive guidance tool](#)

[Legitimate interests](#)

[Legitimate interests assessment](#)

[Guide to Law Enforcement Processing](#)

[Sharing personal data with law enforcement authorities](#)

[Data sharing and re-use of data by competent authorities for non-law enforcement purposes](#)

# Security

## At a glance

Data protection law requires you to process personal data securely, with appropriate organisational and technical measures in place.

The security measures must be “appropriate” to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

You must also take into account the various security measures available and the costs of implementation when determining what measures are appropriate for your circumstances.

## In more detail

- [What does data protection law say about security?](#)
- [Are we still responsible after we've shared the data?](#)

### What does data protection law say about security?

Data protection law requires you to process personal data securely, with appropriate organisational and technical measures in place. The security measures must be “appropriate” to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

This section applies to processing both under the UK GDPR/Part 2 of the DPA 2018 and Part 3 of the DPA 2018.

You must also take into account the various security measures available and the costs of implementation when deciding what measures are appropriate for your circumstances. The “data protection by design and default” approach described in the section on accountability will help you to consider the security measures to put in place.

As stated earlier, you should aim to build a culture of compliance and good practice throughout your organisation to help you to share data securely. This must apply from board level, through to all employees and contractors.

For more details, please see the guidance on security on the ICO website.

### Are we still responsible after we've shared the data?

Organisations that you share data with take on their own legal responsibilities for the data, including its security. However you should still take reasonable steps to ensure that the data you share will continue to be protected with adequate security by the recipient organisation. You should:

- ensure that the recipient understands the nature and sensitivity of the information;
- take reasonable steps to be certain that security measures are in place, particularly to ensure that you have incorporated an agreed set of security standards into your data sharing agreement, where you have one; and

- resolve any difficulties before you share the personal data in cases where you and the recipient organisation have different standards of security, different IT systems and procedures, different protective marking systems etc.

Undertaking a DPIA for any data sharing operation can be an effective means of considering these issues and implementing appropriate mitigating measures.

You should also note that in certain circumstances you are required to do a DPIA when sharing data, and we recommend that you always do so when planning to share data. Please refer to the [section in this code on Deciding to share data](#).

## Further Reading

[↗ Relevant provisions in the legislation - see UK GDPR Articles 5.1\(f\), 32, 35 ↗](#)

External link

[↗ Relevant provisions in the legislation - see UK GDPR Recitals 39, 83 ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 section 40 \(law enforcement processing\) ↗](#)

External link

### Further reading

[Guidance on security](#)

[Guidance on data protection by design and default](#)

The ICO has also worked closely with the National Cyber Security Centre (NCSC) to develop a set of [security outcomes](#) that you can use to help determine what's appropriate for you. The security outcomes can also help you when considering any data sharing arrangements.

# The rights of individuals

## At a glance

In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights easily.

There are additional requirements if your data sharing involves automated decision-making.

The position on individual rights is slightly different for law enforcement processing.

## In more detail

- [What is the impact of the rights of individuals on data sharing?](#)
- [How do we allow individuals to exercise their information rights in a data sharing scenario under the UK GDPR?](#)
- [What is the impact on a data sharing arrangement of requests for erasure, rectification or the restriction of processing?](#)
- [How do we deal with complaints and queries from individuals about sharing their data?](#)
- [What do we need to do if the data sharing involves solely automated processing?](#)
- [What do we need to do if the data sharing involves automated decision-making or profiling that does not fall within Article 22 UK GDPR?](#)
- [What individual rights are provided by Part 3 of the DPA 2018: law enforcement processing?](#)

## What is the impact of the rights of individuals on data sharing?

In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights.

The rights available to an individual data subject under the UK GDPR and under Part 3 of the DPA 2018 (law enforcement processing) differ in some respects. Please see the paragraph below on individual rights under Part 3 for law enforcement processing.

The UK GDPR gives individuals specific rights over their personal data. For general data processing under the UK GDPR, in summary these are:

- the right to access personal data held about them (the right of subject access);
- the right to be informed about how and why their data is used - and you must give them privacy information;
- the rights to have their data rectified, erased or restricted;
- the right to object;
- the right to portability of their data; and
- the right not to be subject to a decision based solely on automated processing.

There are exemptions and restrictions that can, in some circumstances, be legitimately applied to exempt

or qualify the right of individuals to exercise their rights.

This section of the code does not seek to replicate existing ICO guidance on individual rights, but rather focuses on how the rights impact on data sharing. You should refer to guidance on the ICO website for more details.

## How do we allow individuals to exercise their information rights in a data sharing scenario under the UK GDPR?

- You must have policies and procedures that allow individuals to exercise their rights easily, and you must set these out in your data sharing agreement.
- If you are a joint controller, these should be set out clearly in the transparent arrangement you and your other joint controller or controllers are required to enter into under Article 26 of the UK GDPR (for law enforcement processing, it is set out in section 58 in Part 3 of the DPA 2018).
- You must provide details of how to exercise these rights in the privacy information you issue to individuals.
- You must make the exercise of individual rights as straightforward as possible. Be aware that although your DPO may be the first point of contact, individuals may contact any part of your organisation.
- Where several organisations are sharing data, it may be difficult for an individual to decide which organisation they should contact. You should make that clear in the privacy information you provide to them at the time you collect their data, as well as in any transparent arrangement made under Article 26.
- In a data sharing arrangement it is good practice to provide a single point of contact for individuals, which allows them to exercise their rights over the data that has been shared without making multiple requests to several organisations. However, they are permitted to choose to exercise their rights against any controller they wish.

### Example

A social sector organisation providing childcare services held information shared from a local authority and the NHS. The Article 26 transparency arrangement set out a clear procedure that whichever organisation received a request for personal data should take a lead on providing the data and notify the other parties if necessary.

The arrangement also set out procedures for how to deal with the exercising of other individual rights.

The procedures were also provided in privacy information given to service users and contained in a data sharing agreement published on the respective organisations' websites.

## What is the impact on a data sharing arrangement of requests for erasure, rectification or the restriction of processing?

Under Articles 16, 17 and 18 of the UK GDPR, data subjects have a right to request erasure, rectification of their data, or the restriction of processing of their data. As with other individual rights, it will be easier for you and for the other organisations in a data sharing arrangement if you have clear policies and procedures

about how to handle such requests.

Under Article 19 of the UK GDPR, if you have shared information with other organisations you must inform them of the rectification, erasure or restriction of the personal data, unless this proves impossible or involves disproportionate effort. If asked, you must also inform the individual about those organisations that you have shared their data with.

## How do we deal with complaints and queries from individuals about sharing their data?

Individual data subjects may have queries or complaints about the sharing of their personal data, particularly if they think the data is wrong or that the sharing is having an adverse effect on them.

The way you handle these queries and complaints makes a difference both to the individuals and to your organisation. It is not always a case of simply providing a response. The comments you receive might be an invaluable resource for you when you are reviewing your data sharing arrangement.

It is good practice to:

- have procedures to deal with any complaints and queries in a quick and helpful way;
- provide a single point of contact for complainants or enquirers;
- review the comments (good and bad) you receive in order to obtain a clearer understanding of public attitudes to the data sharing you carry out;
- take the opportunity to provide individuals with information about your data sharing, further to that contained in your privacy information, when answering their specific queries;
- use any significant objections, negative comments or other expressions of concern you receive when you inform people about your data sharing, to help you review your data sharing: the amount of data you share, or which organisations you share it with. You may need to decide whether the sharing can go ahead in the face of public opposition. For example, you might decide to go ahead because you are under a legal obligation to share the data; and
- consider setting up focus groups to explore individuals' concerns, if you are carrying out large-scale data sharing operations.

## What do we need to do if the data sharing involves solely automated processing?

Article 22 of the UK GDPR gives data subjects additional protective rights if your data sharing arrangement involves solely automated processing:



“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

“Solely” here means that there is no human influence on the outcome.

### **Example of solely automated decision-making**



A bank made a decision not to grant a loan to an individual:

- based on personal data obtained about the individual from a range of sources; and
- using algorithms, rather than the decision-making input of a member of bank staff.

If your data sharing arrangement involves any automated decision-making, including profiling, you must document the specific lawful basis for that in your data protection policy.

Documenting your processing activities will help you to decide whether they constitute profiling and solely automated decision-making.

Processing involving automated processing and profiling has a high level of risk. The UK GDPR requires you to carry out a DPIA in respect of processing that meets the Article 22 definition, to show you have considered the risks and how you will deal with them.

The UK GDPR allows you to carry out processing falling within Article 22, so long as you can rely on one of three exceptions:

- When the decision is necessary for a contract.
- When the decision is authorised by domestic law.
- When the decision is based on the individual's specific consent.

In respect of any processing that falls within Article 22 you must also:

- give individuals specific information about the processing;
- explain to them their rights to challenge a decision and request human intervention; and
- ensure you have measures in place to prevent errors, bias and discrimination in your systems.

Where the processing includes profiling, you must tell individuals that they have a right under Article 21 of the UK GDPR to object to it in certain circumstances.

**What do we need to do if the data sharing involves automated decision-making or profiling that does not fall within Article 22 of the UK GDPR?**

If your data sharing arrangement features automated decision-making or profiling, but does not fall within Article 22, it is still good practice to tell individuals about it; this will help you to meet your transparency obligation. Think carefully about what they would expect you to do with their data.

You must still comply with UK GDPR principles, document your lawful basis and allow individuals to exercise their rights easily.

You must also tell individuals that they have a right under Article 21 of the UK GDPR to object to profiling in certain circumstances.

All automated decision-making or profiling of special category data and of children's personal data has additional protections.

**What individual rights are provided by Part 3 of the DPA 2018: law enforcement processing?**

The individual rights are:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision-making.

Certain rights under the UK GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the DPA 2018. As with the UK GDPR, there are also exemptions and restrictions that can, in some circumstances, be legitimately applied to exempt or qualify the exercise of individuals' rights.

## Further Reading

 [Relevant provisions in the legislation - see UK GDPR Articles 16-19 and 22](#) 

External link

 [Relevant provisions in the legislation - see DPA 2018 Part 3](#) 

External link

### Further reading

[Guidance on the rights of individuals](#)

[Individual rights under the law enforcement processing provisions](#)

[Guidance on exemptions](#)

# Law enforcement processing

## At a glance

Most data sharing, and the bulk of this code, is covered by the general processing provisions under the UK GDPR and Part 2 of the DPA 2018. However, data sharing by a “competent authority” for specific law enforcement purposes is subject to a different regime under Part 3 of the DPA 2018 for law enforcement processing.

If you are a competent authority, it is very likely that you will also be processing personal data for general purposes under the UK GDPR/Part 2 of the DPA 2018, eg for Human Resources matters or other non-law enforcement purposes. In that instance, you should follow the general sections of the code on UK GDPR/Part 2 data sharing.

## In more detail

- [Introduction](#)
- [What is a competent authority?](#)
- [What are the law enforcement purposes?](#)
- [We are a competent authority: how do we share data under Part 3 of the DPA 2018?](#)
- [We are a competent authority: how do we share data with a controller that is not a competent authority?](#)
- [We are not a competent authority: how do we share data with a competent authority?](#)
- [How do we allow individuals to exercise their information rights under Part 3?](#)
- [How do we comply with the accountability requirement under Part 3?](#)

## Introduction

There are compelling reasons why data sharing is needed for law enforcement purposes. We are aware that sometimes organisations are hesitant about data sharing in this context. However, we emphasise that data protection law does not prevent appropriate data sharing when it is necessary to protect the public, to support ongoing policing activities, or in an emergency for example. Adhering to the provisions of the legislation and following the good practice set out in this code will help you to share data in a compliant and proportionate way.

Most data sharing, and hence the bulk of the code, is covered by the general processing provisions under Part 2 of the DPA 2018; in practice, this means referring to the UK GDPR. Data sharing by a **competent authority** for specific **law enforcement purposes** is subject to a different regime under Part 3 of the DPA 2018, which provides a separate but complementary framework. However, there are common elements to both regimes which means that data sharing processes under either Part 2 or Part 3 can be adapted, rather than having to start a new process.

### Example

Requests for information made by competent authorities must be reasonable in the context of their law enforcement purpose, and the necessity for the request should be clearly explained to the organisation.

For example, the police might ask a social worker to pass on case files to them containing details of young teenagers who may be at risk of exploitation.

The social worker might feel reluctant to voluntarily disclose information to the police if the request appears excessive, or the necessity or urgency appears unjustified. The police should provide as much clarity as they can about their lines of enquiry, without prejudicing their investigation.

## What is a competent authority?

A competent authority is:

- a person specified in Schedule 7 of the DPA 2018; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes (section 30(1)(b) of the DPA 2018).

You need to check whether you are listed as a competent authority in Schedule 7 of the DPA 2018. The list includes most government departments, police chief constables, the Commissioners of HMRC, the Parole Boards and HM Land Registry.

If you are not listed in Schedule 7, you may still be a competent authority if you have a legal power to process personal data for law enforcement purposes. For example, local authorities who prosecute trading standards offences, or the Environment Agency when prosecuting environmental offences.

## What are the law enforcement purposes?

This term is defined in section 31 of the DPA 2018 as:



“the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”

Criminal law enforcement must be the primary purpose of the processing.

Even if you are a competent authority, it is very likely that you will also be processing personal data for general purposes under the UK GDPR/Part 2 of the DPA 2018, rather than for law enforcement purposes. An example might be for Human Resources matters. In that instance, you should follow the general data sharing guidance contained elsewhere in this code; we also refer to this below.

## We are a competent authority. How do we share data under Part 3 of the DPA 2018?

If you are a competent authority, and the sharing is to another competent authority for law enforcement

purposes, then Part 3 should provide a framework allowing you to share data.

This differs in some ways from the general processing provisions in the UK GDPR and Part 2 of the DPA 2018. The differences, including lawful basis, are primarily because of the purpose for which you are processing the data.

In particular, there are some differences in the principles in Part 3, and processing of data described in Part 3 as “sensitive” is subject to additional safeguards, such as conditions in Schedule 8 of the DPA 2018. You can find out more about the requirements on the ICO website.

**We are a competent authority. How do we share data with a controller that is not a competent authority?**

### **Part 3 to Part 2 DPA 2018 data sharing**

A common scenario here is data sharing by a competent authority (that is processing for law enforcement purposes) to a recipient where the disclosure is not for law enforcement purposes, or the recipient is not a competent authority. In practice, Part 3 DPA 2018 information may be shared with a third party or repurposed internally, and then be used for general processing purposes under the UK GDPR and Part 2 of the DPA 2018.

- Section 36(4) of the DPA 2018 allows you to do this, provided that “the processing is authorised by law”.
- As a competent authority, you must determine whether any processing of such data for non-law enforcement purposes is “authorised by law”. This might be, for example, statute, common law, royal prerogative or statutory code.
- The question of “authorised by law” will, in part, depend on the specific laws to which the relevant competent authority is subject. For some authorities (such as the police), you may be able to rely more heavily on common law than other organisations that are more constrained by the nature of their constitution and legal framework. These would include local authorities, which may only do those things that they are empowered to do by statute, or those that are reasonably ancillary or incidental to those powers.
- You should start by identifying the reason and the lawful basis for the sharing.
- If you are the police you should also take into account the relevant policing purposes. In the absence of a clear policing purpose, it may be that the Part 3 DPA 2018 personal data/police information should not be disclosed. See more on this below. You should then identify a relevant processing condition under the UK GDPR/Part 2 of the DPA 2018.

For the police, in the absence of an obvious statute or code of practice to provide authorisation, common law may be the natural basis to rely upon. However, as recognised by the College of Policing, common law does not provide the police with an unconditional power to engage in any activity that is not otherwise provided for by statute. It cannot be used in a way that contravenes or conflicts with any legislation, and actions based on common law must still be compliant with the Human Rights Act 1998 and the DPA 2018.

#### **Example**

The police may provide information to the civil courts about child protection proceedings. Both the police and the court are competent authorities, but since the court proceedings are civil rather than criminal, the disclosure by the police is not in the context of law enforcement purposes. This is the

case even though the reason for the police disclosing the information is to protect life, which is a policing purpose.

We are not a competent authority. How do we share data with a competent authority?

### **Part 2 to Part 3 DPA 2018 data sharing**

If you are an organisation that does not fall within the DPA 2018 definition of a competent authority, then you can share data for law enforcement purposes with a competent authority, such as the police, in compliance with the UK GDPR and Part 2 of the DPA 2018. However, you must still have a lawful basis under Article 6 for the sharing; for example, legitimate interests. Where a request has come from a law enforcement agency under the Investigatory Powers Act 2016, the lawful basis might be legal obligation. You are also likely to need a condition for disclosing the data under Schedule 1 of the DPA 2018.

Requests for information made to you by competent authorities must be reasonable in the context of their law enforcement purpose, and they should clearly explain the necessity for the request to you.

Where necessary in the circumstances, you can also rely on the "crime and taxation" exemption from some UK GDPR provisions that is set out in DPA 2018 schedule 2, paragraph 2(1). This includes exemption from transparency obligations and most individual rights, to the extent that the application of those provisions is likely to prejudice the prevention or detection of crime.

If you are not a competent authority and are disclosing data about an individual's criminal offences and convictions (including allegations that an individual has committed an offence) you must comply with Article 10 of the UK GDPR.

In practice, this means you need to meet a relevant condition in Schedule 1 of the DPA 2018. In this scenario, the most likely condition is in Schedule 1 paragraph 10, as modified by paragraph 36: disclosures of "criminal offence" data which are necessary for the purposes of the prevention or detection of unlawful acts; and where asking for the individual's consent would prejudice those purposes.

The personal data of witnesses, victims, bystanders and other persons who are not the offender or alleged offender is not "criminal offence" data and a Schedule 1 DPA condition is not required to allow the processing and sharing of their data.

However, if the data you are sharing includes special category data, a condition under Article 9 of the UK GDPR needs to apply, together with a linked condition in Schedule 1 of the DPA 2018 in most cases (most likely Article 9.2(g) together with Schedule 1 paragraph 10 of the DPA 2018). You must be able to demonstrate that sharing the special category data is necessary for reasons of substantial public interest.

The DPA 2018 usually requires organisations to have an appropriate policy document to cover their general data processing under this condition. However, an organisation disclosing data to a competent authority in reliance on the condition in Schedule 1 paragraph 10 of the DPA 2018 does not need to have a policy document to cover that disclosure.

### **Example**

A shopkeeper used CCTV, and routinely captured footage of customers in the premises. A copy of some CCTV footage was requested by a police force for an ongoing criminal investigation. The

police force told the shopkeeper why they wanted it (some competent authorities may use a standard form for this).

The shopkeeper was processing data under the UK GDPR and Part 2 of the DPA 2018. Assuming the shopkeeper had a lawful basis for the processing, they could give the police a copy of the footage to help with the investigation. If the footage included images of an alleged offender they could rely on Schedule 1, paragraph 10 to process the CCTV data, and enable the sharing of the relevant footage with the police to help with the investigation.

The receiving police force (competent authority) was processing the information under Part 3 of the DPA 2018. This enabled them to fulfil their statutory functions.

## How do we allow individuals to exercise their information rights under Part 3?

There are differences in the availability of individual rights for law enforcement processing. Certain individual rights under the UK GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the DPA 2018. There are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights if there is a likely prejudice to the law enforcement purposes.

For further details on this, please refer to [the section in this code on the rights of individuals](#), and to the ICO website guidance on law enforcement processing.

## How do we comply with the accountability requirement under Part 3?

Section 34(2) in Part 3 of the DPA 2018 states that you are responsible for compliance. It requires you, as controller, to demonstrate that you comply with the principles.

You must put in place appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include policies and procedures, including data protection by design and default.

You must also maintain relevant documentation of data processing activities.

Please also see [the earlier section in this code on accountability](#). For more specific details on Part 3 DPA 2018, please refer to the ICO guidance on law enforcement processing.

## Further Reading

[Relevant provisions in the legislation - see UK GDPR Articles 6, 9, 10](#)

External link

[Relevant provisions in the legislation - see UK GDPR Recitals 40, 41, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56](#)

External link

[Relevant provisions in the legislation - see DPA 2018 section 10](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 section 11\(2\) ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 section 15 ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 section 30\(1\)\(b\) ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 section 31 ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 schedule 1 \(paragraphs 10 and 36\) ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 schedule 2 \(paragraph 2\) ↗](#)

External link

[↗ Relevant provisions in the legislation - see DPA 2018 schedule 7 ↗](#)

External link

## Further reading

[Guide to Law Enforcement Processing](#)

[Sharing personal data with law enforcement authorities](#)

[Data sharing and re-use of data by competent authorities for non-law enforcement purposes](#)

[Guide to data protection](#)

[Guidance on exemptions](#)

[Guidance on the appropriate policy document](#)

Further resources and support are available on the ICO [data sharing information hub](#).



# Due diligence

## At a glance

If a merger or acquisition or other change in organisational structure means that you have to transfer data to a different or additional controller, you must consider data sharing as part of the due diligence you carry out when taking on the organisation and its obligations. This includes establishing the purposes for which the data was originally obtained, your lawful basis for sharing it, and whether these have changed following the merger or acquisition.

You must comply with the data protection principles, and document your data sharing.

Consider when and how you will inform individual data subjects about what's happening to their data. You must also ensure sound governance, accountability and security.

## In more detail

- [Introduction](#)
- [How does data sharing apply to mergers and acquisitions?](#)
- [How do we manage shared data following a merger or restructure or other change of controller?](#)

### Introduction

This section is of particular relevance to the private sector. It highlights situations such as mergers and acquisitions, or other changes in organisational structure, where you need to make good data sharing practice a priority.

### How does data sharing apply to mergers and acquisitions?

Data sharing considerations may become a priority when a merger or acquisition or other change in organisational structure means that you have to transfer data to a different organisation. For example, as part of a takeover; or on insolvency, data might be sold as an asset to a different legal personality. You must take care if, as a result of the changes, there is a change in the controller of the data, or if the data is being shared with an additional controller. This is the case whether you are the sharing or recipient controller. You might be an insolvency practitioner or other adviser taking the role of controller for the time being, or advising a different controller. You need to:

- ensure that you consider the data sharing as part of the due diligence you carry out;
- follow this data sharing code;
- establish what data you are transferring;
- identify the purposes for which the data was originally obtained;
- establish your lawful basis for sharing the data;
- ensure you comply with the data processing principles - especially lawfulness, fairness and transparency to start with;
- document the data sharing;

- seek technical advice before sharing data where different systems are involved: there is a potential security risk that could result in the loss, corruption or degradation of the data; and
- consider when and how you will inform data subjects about what is happening. Under the UK GDPR you are required to keep individual data subjects informed about certain changes relating to the processing of their data, and they may have a right to object. Please see the guidance on individual rights on the ICO website. The same considerations may apply in reverse to the controller receiving the data.

## How do we manage shared data following a merger or restructure or other change of controller?

On a practical level, it can be difficult to manage shared data immediately after a change of this kind, especially if you are using different databases, or you are trying to integrate different systems. It is particularly important in this period to consider the governance and accountability requirements of the UK GDPR. You must:

- check that the data records are accurate and up to date;
- ensure you document what you do with the data;
- adhere to a consistent retention policy for all records; and
- ensure appropriate security is in place.

## Further Reading

 [Relevant provisions in the legislation - see UK GDPR Articles 5, 6, 7 and 21](#) 

External link

 [Relevant provisions in the legislation - see UK GDPR Recitals 39, 40, 42, 43, 50, 69, 70](#) 

External link

### Further reading

Guidance on [individual rights under the UK GDPR](#)

# Sharing personal data in databases and lists

## At a glance

The transfer of databases or lists of individuals is a form of data sharing, whether for money or other consideration, and whether for profit or not.

It is your responsibility to satisfy yourself about the integrity of the data supplied to you.

You are responsible for compliance with the law for the data you receive, and you have to respond to any complaints about it.

## In more detail

- [How does data sharing apply to the acquisition or transfer of databases and lists?](#)
- [What must we do to ensure the database or list we are receiving is being shared in compliance with the law?](#)
- [What else do we need to do?](#)
- [How does data sharing interact with direct marketing?](#)
- [How does data sharing interact with political campaigning?](#)

## How does data sharing apply to the acquisition or transfer of databases and lists?

The transfer of databases or lists of individuals is a form of data sharing, whether for money or other consideration, and whether for profit or not. This section considers data sharing which has not resulted from organisational changes.

Examples of organisations involved in this type of data sharing may include:

- data brokers;
- credit reference agencies;
- marketing agencies;
- franchised businesses;
- separate parts of a business that operate independently from their head office;
- clubs and societies;
- charities and voluntary groups; and
- political parties.

Please note that some of these examples may involve transfers between controllers and processors and are therefore outside the scope of this code.

You will find it beneficial to follow the good practice set out in this code. The due diligence carried out by both the sharing and recipient controllers is crucial to compliance.

We will look at this from the viewpoint of the organisation receiving the database or list. The organisation

sharing the data should follow a similar process.

## What must we do to ensure the database or list we are receiving is being shared in compliance with the law?

It is your responsibility to satisfy yourself about the integrity of the data supplied to you. You are responsible for compliance with the law for the data you receive, and you have to respond to any complaints about it. You should make appropriate enquiries and checks, including the following:

- confirm the source of the data;
- identify the lawful basis on which it was obtained and that any conditions about that lawful basis were complied with;
- check what individuals were told at the time of handing over their data;
- verify details of how and when the data was initially collected;
- check the records of consent, if you are relying on consent;
- review a copy of the privacy information given at the time of collection of the data;
- check what information was given to individuals in accordance with Article 14 of the UK GDPR - ie privacy information that must be given when data is obtained from a source other than the data subject;
- check that the data is accurate and up to date; and
- ensure that the data you receive is not excessive or irrelevant for your needs.

It is good practice to have a written contract with the organisation supplying you with the data.

## What else do we need to do?

You must tell data subjects who you are sharing their data with, and for what purposes. Under Article 13 of the UK GDPR you must give privacy information to data subjects at the same time as collecting the data from them. Under Article 14 of the UK GDPR you must give privacy information to individuals whose data has been shared with you indirectly "...within a reasonable period after obtaining the personal data, but at the latest within one month...". There are some exceptions to these requirements; for example, you do not need to provide individuals with information they already have. It is your responsibility on receiving the data to be satisfied that this has been done.

## How does data sharing interact with direct marketing?

If this form of data sharing is relevant to your data sharing arrangement you should read the ICO's detailed guidance on direct marketing.

## How does data sharing interact with political campaigning?

Political parties, referendum campaigners and candidates use information about voters to help them target their campaign materials more effectively and to raise funds. They may:

- buy lists and databases from organisations such as data brokers; and
- use third parties to send out campaign materials.

This may involve data sharing. Communicating with voters, such as via social media platforms and

targeting political messages, may also amount to direct marketing.

You should carry out the checks described earlier in this section in order to satisfy yourself about the integrity of the data supplied to you.

If you use a third-party organisation to send out campaign materials on your behalf using your database, you may be sharing data with that external organisation, which is either a controller or a processor. For the purposes of this code, if you are both controllers you should still be careful to check and monitor what the third party is doing. You are responsible as controller(s) for that data and for compliance with the law. You should read and follow the ICO guidance on the law about both political campaigning and direct marketing.

## Further Reading

 [Relevant provisions in the legislation - see UK GDPR Articles 13 and 14](#) 

External link

### Further reading

See the Direct marketing code and guidance on the ICO website [www.ico.org.uk](http://www.ico.org.uk)

See the Political campaigning guidance on the ICO website [www.ico.org.uk](http://www.ico.org.uk)

See the [Guide to Privacy and Electronic Communications Regulations \(PECR\)](#)

# Data sharing and children

## At a glance

If you are considering sharing children's personal data, you must take extra care.

You may share children's personal data as long as you can demonstrate a compelling reason to do so, taking account of the best interests of the child. The best interests of the child should be a primary consideration.

You should build all this into the systems and processes in your data sharing arrangement. A high level of privacy should be your default.

Sharing children's data with third parties can expose them to unintended risks if not done properly.

You should carry out a DPIA to assess and mitigate risks to the rights and freedoms of children, which arise from your data sharing.

## What do we need to bear in mind when sharing children's data?

The best interests of the child should be a primary consideration. This concept comes from the United Nations Convention on the Rights of the Child (UNCRC), which declares that "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration." In essence, the best interests of the child are whatever is best for that individual child.

Things you should consider:

- You may share children's personal data as long as you have a compelling reason to do so, taking account of the best interests of the child. One clear example of a compelling reason is data sharing for safeguarding purposes; another is the importance for official national statistics of good quality information about children. However, selling on children's personal data for commercial re-use is unlikely to amount to a compelling reason for data sharing. Even if you have a compelling reason for sharing children's personal data, you must still carry out a DPIA, because children are a vulnerable group.
- Use a DPIA to assess and mitigate risks to the rights and freedoms of children, which arise from your data sharing.
- You have to balance the best interests of the child against the rights of others. For example, it is unlikely that the commercial interests of an organisation will outweigh a child's right to privacy.
- Considering the best interests of the child should form part of your compliance with the lawfulness, fairness and transparency requirements. Is it fair to share the child's data? What is the purpose of the sharing?
- Children are less aware than adults of the risks involved in having their data collected and processed, so you have a responsibility to assess the risks and put appropriate measures in place. Where appropriate, consider children's views when designing your data sharing arrangement.
- Children's vulnerability means that the risks in sharing their data may be higher than in the similar processing of adults' data.
- The privacy information you provide must be clear and presented in plain, age-appropriate language.

- You should carry out due diligence checks on the organisations with which you are planning to share data. You should consider what the organisation you are sharing the data with plans to do with it. If you can reasonably foresee that the data will be used in a way that is detrimental to the child, or otherwise unfair, then you shouldn't share.
- You should ensure that any default settings relating to data sharing specify the purpose of the sharing and who the data will be shared with. Settings which allow general or unlimited sharing are not compliant.
- Consent is not the only lawful basis to use. Other lawful bases might be more appropriate.
  - If you are relying on consent, you must consider the competence of the child to give their own consent, and whether that consent is freely given (eg where there is an imbalance of power).
  - You should also consider the child's competence if you are relying on the lawful basis that the sharing is necessary for the performance of a contract.
- If you (or another data controller in the data sharing arrangement) are a provider of an online service likely to be used by children then you also need to conform to the Age Appropriate Design Code.

## Further Reading

 [Relevant provisions in the legislation - see UK GDPR Articles 6.1, 8, 12.1 and Recitals 38, 58, 65, 71, 75](#)  
External link

### Further reading

[Guide to data protection: children](#)

[Children and the UK GDPR](#)

[Age Appropriate Design Code](#)

[Children's code hub](#)

[United Nations Convention on the Rights of the Child](#)

# Data sharing in an urgent situation or in an emergency

## At a glance

In an emergency you should go ahead and share data as is necessary and proportionate.

An example of an emergency situation is the risk of serious harm to human life.

You should plan ahead for urgent or emergency situations as far as possible.

## In more detail

- [What should we do in an urgent or emergency situation?](#)
- [How can we plan ahead for data sharing in urgent or emergency situations?](#)

Much of this code envisages that you are carrying out data sharing on a routine basis and that you have the opportunity and time to plan carefully ahead. However this might not always be the case.

## What should we do in an urgent or emergency situation?

Urgent or emergency situations can arise that you may not have envisaged, and you have to deal with them on the spot.

In an emergency, you should go ahead and share data as is necessary and proportionate. Not every urgent situation is an emergency. An emergency includes:

- preventing serious physical harm to a person;
- preventing loss of human life;
- protection of public health;
- safeguarding vulnerable adults or children;
- responding to an emergency; or
- an immediate need to protect national security.

Tragedies over recent years such as the Grenfell Tower fire, individual instances of self-harm, major terrorist attacks in London and Manchester, and the crisis arising from the coronavirus pandemic have illustrated the need for joined-up public services responses where urgent or rapid data sharing can make a real difference to public health and safety. In these situations, it might be more harmful not to share data than to share it. You should factor in the risks involved in not sharing data to your service.

## How can we plan ahead for data sharing in urgent or emergency situations?

In an urgent or emergency situation, you have to take decisions rapidly. Often, forward planning helps. In the same way as emergency services plan for various scenarios, you should plan ahead for your organisation and train your staff accordingly. In urgent or emergency situations, when there is less time to



consider issues in detail, it can be particularly difficult to make sound judgements about whether to share information.

Likewise, there can be reasons why organisations and agencies are hesitant about the concept of sharing information when carrying out emergency planning, or about sharing it in the recovery phase of an incident, where the need to share information may appear less urgent.

The key point is that the UK GDPR and the DPA 2018 do not prevent you from sharing personal data where it is appropriate to do so. It is particularly relevant to factor into your considerations, training and procedures for this type of situation the risks involved in not sharing data.

Where possible, if you are likely to be involved in responding to emergency or critical situations, you should consider the types of data you are likely to need to share in advance. As part of this it would be useful to consider any pre-existing DPIA, and also refer to your business continuity and disaster recovery plans. As part of your planning, you should bear in mind that criminals might use a major incident or crisis as an opportunity to try to obtain personal data unlawfully. Therefore, the security measures outlined earlier in this code still remain relevant and necessary in times of urgent sharing.

All this should help you to establish what relevant data you hold, and help to prevent any delays in an emergency or crisis situation.

All types of organisations might have to face an urgent but foreseeable situation, so you should have procedures about the personal data you hold and whether, and how, you should share any of this information. As part of your accountability duty, you should document the action you took after the event, if you can't do it at the time.

### **Example**

The police, the fire service and local councils met to plan for identifying and assisting vulnerable people in their area in an emergency situation such as a flood or major fire. As part of the process, they determined what type of personal data they each held and had a data sharing agreement to set out what they would share and how they would share it in an emergency.

They reviewed this plan at regular scheduled intervals.

### **Further information**

The ICO's [Data protection and coronavirus information hub](#)

# Data sharing across the public sector: the Digital Economy Act codes

## At a glance

The government has devised a framework for sharing personal data, for defined purposes across specific parts of the public sector, under the Digital Economy Act 2017 (DEA).

The aim is to improve public services through the better use of data, while ensuring privacy, clarity and consistency in how the public sector shares data.

## In more detail

- [Data sharing under the Digital Economy Act 2017](#)
- [The Framework for data processing by government](#)

## Data sharing under the Digital Economy Act 2017

The government introduced a framework for sharing personal data for defined purposes across specific parts of the public sector, under the Digital Economy Act 2017 (DEA): the DEA framework.

Its aims are to:

- ensure clarity and consistency in how the public sector shares personal data;
- improve public services through the better use of data; and
- ensure data privacy.

The government has also made it clear that you should only share data when there is a clear public benefit.

Part 5 of the DEA focuses on digital government, providing gateways that allow specified public authorities to share data with each other. Some of these gateways enable the sharing of personal data, while others allow the sharing of non-identifying data. The objectives and purposes for data sharing under the DEA powers are tightly defined.

Under the DEA you must still comply with the data protection legislation.

Part 5 of the DEA explicitly:

- states that all processing of information under the DEA powers must comply with data protection legislation; and
- prohibits the disclosure of information where it would contravene data protection legislation.

Note that although the DEA pre-dates the coming into force of the EU GDPR and of the UK GDPR, it was drafted with a view to being consistent with EU GDPR provisions, as these were already known following agreement of the EU GDPR text in 2016.

The powers to share information under Part 5 of the DEA are supplemented by statutory codes of practice (the DEA codes) which must be consistent with the Information Commissioner's data sharing code of

practice “as altered or replaced from time”. The DEA codes must follow the data protection principles, ensuring that sharing personal data under the DEA powers is proportionate.

For example, there is a DEA code for public authorities sharing personal data about aspects of public service delivery. Its purpose is to achieve specified public service delivery objectives:

- to assist people experiencing multiple social or economic disadvantages, or living in fuel or water poverty;
- to reduce and manage debt owed to the public sector; and
- to combat fraud against the public sector.

There are also provisions in the DEA facilitating data sharing by and with the Statistics Board to allow the production of statistics, disclosure of information by civil registration officials, disclosure of information by Revenue Authorities, and data sharing for research purposes.

The DEA does not currently cover data sharing relating to the provision of health and social care.

The DEA codes contain guidance about what data you can share and for which purpose. They include safeguards to make sure that the privacy of citizens’ data is protected. The two DEA codes that cover public service delivery, debt and fraud powers, and civil registration powers, require public authorities to put in place a data sharing or information sharing agreement, and specify what the agreement must cover.

Anyone who discloses information under the DEA Part 5 powers must also “have regard” to other codes of practice issued by the Information Commissioner. This is in “so far as they apply to the information in question”:

- on the identification and reduction of risks to privacy of a proposal to disclose information; and
- on the information to be provided to individuals about how information collected from them will be used.

## The Framework for data processing by government

Section 191 of the DPA 2018 confers a discretionary power on the Secretary of State to publish a Framework for Data Processing by Government. The DEA framework is separate from this, but the expectation is that any government Framework will be consistent with the data sharing code and any future guidance published by government.

## Further Reading

 [Relevant provisions in the legislation - Digital Economy Act 2017](#) 

External link

### Further reading

[Digital Economy Act Part 5 Codes of practice](#) 

# Enforcement of this code

## At a glance

The ICO upholds information rights in the public interest. In the context of data sharing, our focus is to help you carry out data sharing in a compliant way.

We have various powers to take action for a breach of the GDPR or DPA 2018. We will always use our powers in a targeted and proportionate manner, in line with our regulatory action policy.

## In more detail

- [What is the role of the ICO?](#)
- [How does the ICO monitor compliance?](#)
- [How does the ICO deal with complaints?](#)
- [What are the ICO's enforcement powers?](#)

### What is the role of the ICO?

The ICO is the independent supervisory authority for data protection in the UK.

Our mission is to uphold information rights for the public in the digital age. Our vision for data protection is to increase the confidence that the public have in organisations that process personal data. We offer advice and guidance, promote good practice, monitor and investigate breach reports, monitor compliance, conduct audits and advisory visits, consider complaints and take enforcement action where appropriate. Our enforcement powers are set out in Part 6 of the DPA 2018.

We have also introduced initiatives such as the Sandbox to support organisations using personal data to develop innovative products and services.

Where the provisions of this code overlap with other regulators, we will work with them to ensure a consistent and co-ordinated response.

### How does the ICO monitor compliance?

We use this code in our work to assess the compliance of controllers through our audit programme and other activities.

Our approach is to encourage compliance. Where we do find issues, we take fair, proportionate and timely regulatory action to guarantee that individuals' information rights are properly protected.

### How does the ICO deal with complaints?

If someone raises a concern with us about your data sharing, we will record and consider their complaint.

We will take this code into account when considering whether you have complied with the UK GDPR or DPA 2018, particularly when considering questions of fairness, lawfulness, transparency and accountability.

We will assess your initial response to the complaint, and we may contact you to ask some questions and give you a further opportunity to explain your position. We may also ask for details of your policies and procedures, your DPIA, and other relevant documentation. We expect you to be accountable for how you meet your obligations under the legislation, so you should make sure that when you initially respond to complaints from data subjects you do so with a full and detailed explanation about how you use their personal data and how you comply.

If we consider that you have failed (or are failing) to comply with the GDPR or the DPA 2018, we have the power to take enforcement action. We may require you to take steps to bring your operations into compliance or we may decide to fine you, or both.

However, it should be noted that the ICO prefers to work with organisations to find a resolution. Organisations that recognise and take ownership for the correction of shortcomings through the development of a performance improvement plan can avoid formal enforcement action.

## What are the ICO's enforcement powers?

We have various powers to take action for a breach of the UK GDPR or DPA 2018.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, we have the power to issue fines of up to £17.5 million or 4% of your annual worldwide turnover, whichever is higher.

In line with our regulatory action policy, we take a risk-based approach to enforcement. Our aim is to create an environment within which, on the one hand, data subjects are protected, while ensuring that organisations are able to operate and innovate efficiently in the digital age. We will be as robust as we need to be in upholding the law, while ensuring that enterprise is not constrained by red tape, or by concern that sanctions will be used disproportionately. The ICO focuses the use of its enforcement powers on cases involving reckless or deliberate harms, and is therefore unlikely to take enforcement action against any organisation genuinely seeking to comply with the provisions of the legislation. Nor does it seek to penalise organisations where a member of staff has made a genuine mistake when acting in good faith and in the public interest; for example in an emergency situation, or to protect someone's safety.

In an emergency situation, as previously explained, our approach will be proportionate.

These powers are set out in detail on the ICO website.

## Further Reading

[Relevant provisions in the legislation - see UK GDPR Articles 12-22](#)

External link

[Relevant provisions in the legislation - see UK GDPR Recitals 58-72](#)

External link

[Relevant provisions in the legislation - see DPA 2018 sections 129-165](#)

External link

[Relevant provisions in the legislation - see DPA 2018 schedule 12](#)

External link

## Further reading

[What we do](#)

[Make a complaint](#)

[Regulatory Action Policy](#)

[The Guide to the Sandbox](#)

# Glossary

This glossary is a quick reference for key terms and abbreviations. It includes links to further reading and other resources which may provide useful context and more detailed information.

Please note, this glossary is not a substitute for reading the data sharing code, the ICO's guidance, and associated legislation.

Accountability principle	This requires organisations to be responsible for their own compliance with the UK GDPR or DPA 2018, as appropriate, and to demonstrate that compliance.
Anonymisation	<p>The UK GDPR refers to 'Anonymous information'; information that does not relate to an individual, and is therefore is no longer 'personal data' and is not subject to the obligations of the UK GDPR.</p> <p>In order to determine whether data is anonymised you should take into account all the means reasonably likely to be used by a third party to directly or indirectly identify an individual. Please check the ICO website for the most up to date guidance.</p>
Appropriate policy document	An appropriate policy document is a short document outlining your compliance measures and retention policies for special category data. The DPA 2018 says you must have one in place for almost all of the substantial public interest conditions (and also for the employment, social security and social protection condition), as a specific accountability and documentation measure.
Competent authority	A public authority to which Part 3 of the DPA 2018 applies. Competent authorities are defined as those listed in schedule 7 of the DPA 2018, and any other organisation or person with statutory law enforcement functions. For more information, see our <a href="#">Guide to Law Enforcement Processing</a> .
Consent	A freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data. For more information, see our <a href="#">guidance on consent</a> .
Controller	The person (usually an organisation) who decides how and why to process data. For more information, see our <a href="#">guidance on controllers and processors</a> .
Data protection by design and default	A legal obligation requiring organisations to put in place appropriate technical and organisational measures to implement the data protection principles in an effective manner and safeguard individual rights.
Data sharing	Although there is no formal definition of data sharing, the scope of the data sharing code is defined by section 121 of the DPA 2018 as "the disclosure of personal data by transmission, dissemination or otherwise making it available".

Data sharing agreements / protocols	These may be known by different names, but all set out the arrangements and a common set of rules to be adopted by the organisations involved in data sharing.
Data subject	The identified or identifiable living individual to whom personal data relates.
DEA	The Digital Economy Act 2017.
DPA; the DPA 2018	The Data Protection Act 2018, which sits alongside the UK GDPR and sets out the framework for data protection in the UK. For more information, see our guidance: <a href="#">About the DPA 2018</a> .
DPIA	Data Protection Impact Assessment. This is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is <b>likely to result in a high risk</b> to individuals. For more information, see our <a href="#">guidance on DPIAs</a> .
DPO	Data protection officer.
EDPB	European Data Protection Board (formerly the Article 29 Working Party). This is the independent body established by the EU GDPR to ensure consistency within the EU on interpreting the law and taking regulatory action. EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.
Exemptions	The UK GDPR and the DPA 2018 set out exemptions and qualifications to some rights and obligations in some circumstances. For more details, please see our <a href="#">guidance on exemptions</a> and <a href="#">the Guide to Law Enforcement Processing</a> .
Freedom of information legislation	In the UK the main legislation is: Freedom of Information Act 2000 (FOIA), Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information Regulations 2004 (EIR) and the Environmental Information (Scotland) Regulations 2004.
GDPR	The <a href="#">General Data Protection Regulation (EU) 2016/679 (EU GDPR)</a> . Since the UK left the EU, this has been incorporated into UK data protection law as the UK GDPR, which sits alongside the DPA 2018. The EU GDPR may still apply to you if you operate in the European Economic Area (EEA), or monitor the behaviour of individuals in the EEA. For more information, see our guidance <a href="#">Data protection after the end of the transition period</a> and the <a href="#">Guide to Data Protection</a> .
Information Sharing Agreement (ISA)	Another name for a data sharing agreement.
Joint controllers	Where two or more controllers jointly determine the purposes and means of processing. For more information, see our <a href="#">guidance on controllers and processors</a> .



Law enforcement purposes	For Part 3 of the DPA 2018, the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. For more information, see our <a href="#">Guide to Law Enforcement Processing</a> .
Part 2 DPA 2018	This supplements and tailors the UK GDPR for general data processing. For more information, see our guidance <a href="#">About the DPA 2018</a> .
Part 3 DPA 2018	This sets out a separate regime for law enforcement authorities with law enforcement functions (competent authorities) when they are processing data for law enforcement purposes. For more information, see our guidance <a href="#">About the DPA 2018</a> .
Part 4 DPA 2018	This sets out a separate regime for processing, as specified in Part 4, by an intelligence service or by processors acting on their behalf. An intelligence service for the purpose of Part 4 means the Security Service (MI5), the Secret Intelligence Service (commonly known as MI6), and GCHQ.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'). For more information, see our guidance on <a href="#">What is personal data?</a>
Privacy information	The information that organisations need to provide to individual data subjects about the collection and use of their data. For general data processing, this is specified in Articles 13 and 14 of the UK GDPR. For more details, see our guidance on the <a href="#">Right to be informed</a> . For Law Enforcement Processing under Part 3 of the DPA 2018, the provisions are contained in section 44 of the DPA 2018. For more information on that, see the <a href="#">Guide to Law Enforcement Processing: The right to be informed</a> .
Processing	In relation to personal data, this means any operation or set of operations which is performed on it. This includes collecting, storing, recording, using, amending, analysing, disclosing or deleting it.
Processor	A person (usually an organisation) who processes personal data on behalf of a controller. For more information, see the our <a href="#">guidance on controllers and processors</a> .
Pseudonymisation	Data which has undergone pseudonymisation is defined in the UK GDPR as data that can no longer be attributed to a data subject without the use of additional information. You must ensure that the additional information is kept separately, and that appropriate technical and organisational controls are in place to ensure that re-identification of an individual is not possible. Please check the ICO website for the most up to date guidance.
Publication scheme	For public authorities covered by FOIA and FOISA, you must publish certain information proactively in a publication scheme. Guidance is available on the websites of the Information Commissioner and the Scottish Information Commissioner, respectively.
Sensitive processing	This term is used in Part 3 of the DPA 2018 in relation to law enforcement processing. It is defined in section 35(8) of the DPA 2018 as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health; or

(d) the processing of data concerning an individual's sex life or sexual orientation.

This type of data processing needs greater protection. For more information, see the [Guide to Law Enforcement Processing](#).

Special category data

This term is used about general data processing under the UK GDPR and Part 2 of the DPA 2018. It is defined in Article 9.1 of the UK GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of this type of data needs greater protection. For more information, see our guidance on [Special category data](#).

UK GDPR

The UK version of the EU GDPR, as amended and incorporated into UK law from the end of the transition period by the European Union (Withdrawal) Act 2018 and associated [Exit Regulations](#). The government has published a [Keeling Schedule for the UK GDPR](#) which shows the planned amendments.

WP29

Article 29 Working Party (now the European Data Protection Board).

# Annex A: data sharing checklist

This checklist provides a step-by-step guide to deciding whether to share personal data.

You should use it alongside the data sharing code and guidance on the ICO website [ico.org.uk](https://ico.org.uk).

It highlights what you should consider in order to ensure that your sharing complies with the law and meets individuals' expectations.

## Check whether the sharing is justified

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is it fair to share data in this way?
- Is the sharing necessary and proportionate to the issue you are addressing?
- What is the minimum data you can share to achieve the aim?
- Could the objective be achieved without sharing personal data, or by sharing less personal data?
- What safeguards can you put in place to minimise the risks or potential adverse effects of the sharing?
- Is there an applicable exemption in the DPA 2018?

## Consider doing a Data Protection Impact Assessment

Decide whether you need to carry out a DPIA:

- You must do a DPIA for data sharing that is likely to result in a high risk to individuals. This will depend on the nature, scope, context and purposes of the sharing. For more details on this, see the relevant section of this code and guidance on the ICO website [ico.org.uk](https://ico.org.uk).
- For any data sharing plans, you may find it useful to follow the DPIA process as a flexible and scalable tool to suit your project.

## If you decide to share

It is good practice to have a data sharing agreement. As well as considering the key points above, your data sharing agreement should cover the following issues. You should ensure you cover these matters in any event, whether or not you have a formal agreement in place:

- What information will you share?
- Is any of it special category data (or does it involve sensitive processing under Part 3 of the DPA 2018)? What additional safeguards will you have in place?
- How should you share the information?
  - You must share information securely.
  - You must ensure you are giving the information to the right recipient.
- What is to happen to the data at every stage?
- Who in each organisation can access the shared data? Ensure it is restricted to authorised personnel in each organisation.
- What organisation(s) will be involved? You all need to be clear about your respective roles.
- How will you comply with your transparency obligations?
  - Consider what you need to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language.
  - Consider whether you have obtained the personal data from a source other than the individual.
  - Decide what arrangements need to be in place to comply with individuals' information rights. Bear in mind the differences under Part 3 of the DPA 2018, if applicable.
- What quality checks are appropriate to ensure the shared data is accurate and up-to-date?
- What technical and organisational measures are appropriate to ensure the security of the data?
- What common retention periods for data do you all agree to?
- What processes do you need to ensure secure deletion takes place?
- When should regularly scheduled reviews of the data sharing arrangement take place?

## **Accountability principle**

You must comply with the principles; this point focuses on the accountability principle:

- The accountability principle means that you are responsible for your compliance with the UK GDPR or DPA 2018 as appropriate and you must be able to demonstrate that compliance.
- You must maintain documentation for all your data sharing operations.
- This obligation encompasses the requirement to carry out a DPIA when appropriate.
- You must implement a "data protection by design and default" approach, putting in appropriate technical and organisational measures to implement data protection principles and safeguard

individual rights.

- You must ensure that staff in your organisation who are likely to make decisions about sharing data have received the right training to do so appropriately.

## **Decide what your lawful basis is for sharing the data**

Key points to consider:

- What is the nature of the data and the purpose for sharing it, as well as the scope and context?
- Are you relying on legitimate interests as a lawful basis? If so, you must carry out a legitimate interests assessment (LIA).
- Is any of the data either special category data or criminal offence data? If so, you need to identify additional conditions.
- For law enforcement processing under Part 3 of the DPA 2018, please refer to the references throughout the code and in particular to the Part 3 section.

## **Check whether you have the power to share**

Key points to consider:

- What type of organisation you work for. The position is different for the public and private sectors. Please refer to the data sharing code for more details.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share.
- Whether there are any legal requirements that need to be met when sharing the data - such as copyright or a duty of confidence, or any prohibitions.
- Whether there is a legal obligation or other legal requirement about sharing information – such as a statutory requirement, a court order or common law.

## **Document your decision**

Document your data sharing decision and your reasoning – whether or not you share the information.

If you shared information you should document:

- your justification for sharing;

- what information was shared and for what purpose;
- who it was shared with;
- when and how it was shared;
- whether the information was shared with or without consent, and how that was recorded;
- the lawful basis for processing and any additional conditions applicable;
- individuals' rights;
- Data protection impact assessment reports;
- compliance with any DPO advice given (where applicable);
- evidence of the steps you have taken to comply with the UK GDPR and the DPA 2018 as appropriate; and
- where you have reviewed and updated your accountability measures at appropriate intervals.

# Annex B: Data sharing request form template

For use by the organisation making the request for data sharing

Name of organisation

Name and position of person requesting data

If requester is not the data protection officer (DPO) or equivalent, have they been consulted and their views considered?

Date of request

Description of data requested

Data controller relationship:

Joint  Separate

Will we have a data sharing agreement in place?

Yes  No

Purpose of sharing

Does processing involve any special category data  
(or sensitive processing under part 3 DPA 2018)?

Yes  No

Are there any specific arrangements for retention / deletion of data?

Are there any circumstances in the proposed sharing that might result in a risk to individuals?

[Redacted area]

Date(s) provision of data is required

[Redacted area]



# Data sharing decision form template

For use by the organisation taking the decision to share data

Name of organisation receiving request to share data

Name of organisation requesting data

Name and position of person requesting data

Date request received

Description of data requested

Data controller relationship:

Joint  Separate

Will we have a data sharing agreement in place?

Yes  No

Purpose of sharing

Lawful basis for sharing – please state which

Why is sharing 'necessary'?

Are additional conditions met for special category data or criminal offence data sharing (where applicable)?

Are additional provisions met in the case of Part 3 DPA 2018 data sharing?

Which legal power for sharing applies (if relevant)?

Have you considered a DPIA?

DPIA undertaken and outcome (if applicable)

Were views of DPO (or equivalent) considered? (if DPIA not done)

Are there any specific arrangements for retention/deletion of data?

What are the security considerations?

What arrangements are there for complying with individuals' information rights?

Date(s) of requested sharing (or intervals if data is to be shared on a regular basis)

Decision on request

[Redacted area]

Reason(s) for sharing or not sharing

[Redacted area]

Decision taken by (name and position)

[Redacted area]

Signed:

Dated:

[Redacted area]

# Annex C: case studies

## Fairness and transparency

### **Supermarket providing privacy information to customers**

A supermarket held information about its customers through its loyalty card scheme, in-store CCTV and records of payments. The company did not normally disclose any information to third parties, such as for marketing purposes. However, it would do so if the information it held was relevant to a police investigation or in response to a court order, for example.

The supermarket or the loyalty card scheme operator had to give customers privacy information that provided an explanation, in general terms, of the sorts of circumstances in which it would share information about scheme members with a third party, such as the police.

If the supermarket were to disclose information about a particular scheme member to the police, it would not need to inform the individual of the disclosure if this would prejudice crime prevention.

### **Sharing customer details with a credit reference agency**

A mobile phone company decided to share details of customer accounts with a credit reference agency.

It had to inform customers when they opened an account that it would share information with credit reference agencies.

Credit reference agencies need to be able to link records to the correct individual, so the mobile phone company had to ensure it was collecting adequate information to distinguish between individuals; for example dates of birth.

The organisations involved had to put procedures in place to deal with complaints about the accuracy of the information they shared.

### **Duty to process data fairly when carrying out research using shared data**

A university wanted to conduct research into the academic performance of children from deprived family backgrounds in the local area. The university wanted to identify the relevant children by finding out which ones were eligible for Pupil Premium. Therefore it decided to ask all local primary and secondary schools to share this personal data, as well as the relevant children's test results for the previous three years.

The DPA 2018 contains various provisions that are intended to facilitate the processing of personal data for research purposes. However, there is no exemption from the general duty to process the data fairly. Data about families' income levels, or eligibility for benefits, could be inferred from the Pupil Premium status of a child.

In this example, parents and their children might well have objected to the disclosure of this data because they considered it sensitive and potentially stigmatising. Data about a child's academic performance could be considered equally sensitive.

Instead the school could have identified eligible children on the researchers' behalf and contacted their parents, explaining what the research was about and what data the researchers wanted. The school might have wished to obtain parents' consent for sharing the data, but other lawful bases could have been available to it.

Alternatively, the school could have disclosed an anonymous data set, or statistical information, to the researchers.

## Data sharing agreement: accountability

### **Information sharing framework in healthcare**

Healthcare partners in one county decided to develop an information sharing framework to standardise their sharing processes and encourage agencies to share personal data safely. The framework helped their staff to comply with data protection law by sharing information lawfully, securely and confidentially. As a result, they were able to integrate service provision across the county and deliver better care outcomes for their residents. In a key step, partners brought together information governance leads to oversee the changes needed to develop the framework.

Main purposes of the framework were to ensure that:

- people only had to tell their story once and could expect a better service delivery;
- local people had clear guidance about how their information was shared (and in what circumstances their consent might need to be sought to share it);
- professionals had access to the information they needed, when they needed it, to support better outcomes for local people;
- good decision making was supported by an information sharing framework, providing staff with clear direction; and
- unnecessary appointments and admissions could be avoided.

The principles of the framework were to:

- a) identify the appropriate lawful basis for information sharing;
- b) provide the basis for security of information and the legal requirements associated with information sharing;
- c) address the need to develop and manage the use of Information Sharing Agreements (ISAs);
- d) encourage flows of personal data and develop good practice across integrated teams;
- e) provide the basis for county-wide processes which would monitor and review data flows, and information sharing between partner services;
- f) protect partner organisations from unlawful use of personal data; and
- g) reduce the need for individuals to repeat their story when receiving an integrated service.

Key learning from the introduction of the framework

- Staff needed to be empowered to feel confident about sharing information between partners. Senior leaders needed to be visible to give staff the confidence to share patient information.
- Internal culture needed to be supportive. The culture needed to be underpinned by strong values and ethos. It was essential for a learning culture to be developed so that mistakes could be shared and learnt from, rather than brushed aside. This learning included developing formal training for all staff who were using an integrated care record, supported by the framework.
- Transparency needed to be established so that there was a collective understanding of how the data would be shared and by whom. Staff needed to have clarity around their roles and responsibilities and the benefits of sharing information.
- A need to develop a culture of appropriate sharing in plain English. Messages needed to be simplified to avoid confusion, and jargon needed to be reduced.

## Lawful basis; legal obligation; fairness and transparency; individual rights

### **Data sharing required by law**

A local authority was required by law to participate in a nationwide anti-fraud exercise that involved disclosing personal data about its employees to an anti-fraud body. The exercise was intended to detect local authority employees who were illegally claiming benefits that they were not entitled to.

Even though the sharing was required by law, the local authority still had to inform any employees affected that data about them was going to be shared and still had to explain why this was taking place, unless this would have prejudiced proceedings.

The local authority had to say what data items were going to be shared – names, addresses and National Insurance numbers - and to provide the identity of the organisation they would be shared with.

There was no need for the local authority to seek employees' consent for the sharing because the law says the sharing could take place without consent. The local authority also had to be clear with its employees that even if they objected to the sharing, it would still take place.

The local authority had to be prepared to investigate complaints from any employees who believed they had been treated unfairly because, for example, their records had been mixed up with those of an employee with the same name.

### **Considerations for a healthcare data sharing agreement**

Relevant parts of the NHS and social services in a region shared personal information with the region's police force to ensure that mental health service users who were in contact with the police were safeguarded and had access to appropriate specialist support.

The partner organisations had developed a data sharing agreement to support their joint mental health policy. Depending on the circumstances of each case, the lawful basis might have been consent or a

task carried out in the public interest. The data sharing agreement clearly identified the various pieces of law that each partner relied on to specify their public functions and the provisions they needed to meet if relying on consent. As special category data was likely to be necessary for referrals, they also identified Article 9 conditions. The data sharing agreement reminded all parties to maintain the rights and dignity of patients, their carers and families, involving them in risk assessments wherever possible while also ensuring their safety and that of others.

## Fairness and transparency; individual rights

### **A data sharing arrangement in the private sector relating to the use of new software**

A company specialising in both business-to-business and business-to-consumer transactions used a software-as-a-service (“SaaS”) provider to manage client contact information and integrate communications into its operations. The SaaS provider automated the processes and kept all information up to date. To comply with the requirements of the UK GDPR, the company entered into a data sharing agreement with the SaaS provider.

The agreement outlined a number of obligations for the SaaS provider, such as the nature and scope of information that was to be processed and how the parties intended to implement appropriate security measures.

The company ensured its privacy information was up to date and accurately reflected the data sharing arrangement entered into with the SaaS provider. The fair processing information explained who the data was being shared with and for what purposes. The company also made use of a preference management tool, ensuring individuals were able to control non-essential elements of data sharing between the parties.

## Data sharing agreement; accountability; individual rights

### **Public sector bodies sharing data to provide a co-ordinated approach**

Personal information was shared between two councils, their local schools and colleges, housing providers, relevant community organisations, the local job centres and careers service in order to identify young people who already had been or were currently at high risk of disengaging from education, employment or training. By sharing the information, the partner organisations were able to ensure a co-ordinated approach to providing the most appropriate support to the young person to encourage them back into education, work or training.

The partners used a data sharing agreement to set out their purpose, lawful bases and the information to be shared. The agreement included a section on how to handle data subjects’ rights, and agreed shared security standards; the partners also updated their privacy notices. To quality-assure their agreement, they shared it with a regional group of data protection practitioners for feedback. A timescale was also set for the partners to regularly review the agreement to ensure it stayed up to date

and fit for purpose.

## Data sharing under the Digital Economy Act 2017 powers

Both Companies House (CH) and Her Majesty's Revenue and Customs (HMRC) collect annual accounts from businesses. The accounts contain key corporate and financial information about the company, such as the names of company directors or financial reporting figures showing their profit and loss. There is the opportunity, however, for the same company to file a different set of accounts to each of the two organisations. By filing inflated accounts at CH and lower figures at HMRC, they would simultaneously increase their creditworthiness with financial institutions and wider government while also reducing tax liabilities.

Until 2018, restrictions on data sharing had prevented HMRC and CH from sharing company accounts for comparison. With the introduction of the Digital Economy Act 2017, however, a permissive legal gateway was provided to share information to combat fraud.

Prior to sharing information, CH and HMRC met to draw up the governance and processes:

- They would share information as a pilot.
- Both parties designed and agreed a data specification.
- They completed a data protection impact assessment (DPIA) to ensure they considered proportionality and fair processing.
- Both parties signed an information sharing agreement.

HMRC disclosed the first set of company accounts information to CH in October 2018 – the very first transfer of data under the Digital Economy Act powers.

The pilot sought to address the fraud problem through 10 defined data analytics and compliance work streams, each one relating to a mode of behaviour indicating false account filing and fraudulent activity. For the first time, the pilot utilised qualitative analysis to access and compare key words and phrases. Further to this, the pilot also utilised CH back-office data to uncover previously hidden links between companies, combined for the first time with HMRC intelligence.

The data sharing pilot identified around £10m of savings, with upwards of £50m potential annual savings projected if the data share was embedded as business as usual.

In addition, they identified over 3,500 sets of accounts as incorrect at Companies House, thereby improving the integrity of the data held on the register.

## Data sharing for official statistics and analysis: measuring the pay progression and geographical mobility of young workers



Understanding how young people enter the labour market and progress through their early careers helps to highlight disparities in opportunities and shine a light on differing experiences of being in work, incomes and social mobility. The factors that influence labour market and earnings progression, as well as the geographic mobility of workers, had been a long-standing evidence gap in official statistics and analysis.

In 2018, the Office for National Statistics (ONS) brought together data from the 2011 Census with data on earnings and benefits from the Department for Work and Pensions (DWP) and HM Revenue and Customs (HMRC), for the period 2012 to 2016. This new longitudinal study created a dataset of 28 million individual records, allowing for new analysis of how earnings had changed over this period, not previously possible using the traditional survey sources. Only anonymised data was used in the analysis and results were published at an aggregated level, so that individuals could never be identified by ONS analysts undertaking the research or in the published research outputs.

Alongside 2011 Census data on individual and household characteristics, the new dataset drew on local geography information contained in the DWP administrative dataset to produce analysis of the impact of moving home on pay and earnings progression, especially patterns of movement of young people between local authorities and how earnings growth varied depending on the geographical place of origin and different city or regional destinations. While this showed that four in five young people did not move between local authority areas over the period of the study, for those that did move, on average, young people experienced higher earnings growth. Those moving to London experienced the highest average annual growth in earnings (+22%) while those that either did not move local authority or moved elsewhere had much lower earnings growth (+7%).

Further analysis was published as experimental research on the ONS website in [Young People's Earnings Progression and Geographic Mobility](#).

## Data sharing arrangement between sectors to support families

### **Sharing data between a local authority and local NHS trust to provide better early help and support to families**

Families sometimes have hidden needs so don't receive the support they require from public services – or may be receiving support through one organisation for a specific issue, but have other needs too.

A council worked with an NHS trust to establish a data sharing arrangement between the council and health services to help identify children and families who would benefit from receiving co-ordinated and targeted early help for a range of issues they might be facing.

The data sharing arrangement cross-referenced NHS trust and council caseload data and identified children and families who were being supported by the trust, but not by the council's early help services. These families would then be engaged in wider support to address their needs through the Troubled Families Programme. The data would also be used to understand whether families had in fact benefitted from the support they received and to inform future commissioning of services.

Before sharing data, the two organisations worked together to put measures in place to ensure that the data would be protected and shared responsibly:

- A data protection impact assessment, led by the Head of Information Governance and data protection officer (DPO) at the NHS trust, which identified the potential risks to privacy and how those risks would be mitigated.
- An operational agreement setting out the arrangements for the exchange of data, under the overarching information sharing framework signed by the trust and the council.
- A methodology to make sure the minimum amount of data was shared.
- Privacy information.

Organisations involved: Children's public health, Health Visiting, and Child and Adolescent Mental Health Services (CAMHS); the council and local NHS trust.