Data protection

Data sharing code of practice

Draft code for consultation

Information Commissioner's Office

Data sharing: a code of practice

Contents

Foreword

A foreword by Information Commissioner Elizabeth Denham will be included in the final version of the code.

Summary

- 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 legislation. It explains the law and provides good practice recommendations. Following it along with other ICO guidance will help you to: manage risks; meet high standards; clarify any misconceptions your organisation may have about data sharing; and give you confidence to share data appropriately and correctly.

- This code covers the sharing of personal data between organisations which 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, data can be shared in an urgent or emergency situation.

- When considering sharing data, you must assess your overall compliance with the data protection legislation. As a first step you should decide whether you need to carry out a Data Protection Impact Assessment (DPIA). We recommend you consider following the DPIA process, even where you are not legally obliged to carry one out.

- It is good practice to have a data sharing agreement. It sets out the purpose of the data sharing, covers what is to happen to the data at each stage, sets standards and helps all the parties to be clear about their respective roles. It helps you to demonstrate your accountability under the GDPR.

- When sharing data, you must follow the key principles in data protection legislation.

- The accountability principle means that you are responsible for your compliance with the GDPR or DPA, as appropriate. You must be able to demonstrate that compliance.

- You must identify at least one lawful basis for sharing data from the start.

- You must always share personal data fairly and in a transparent manner. When you share data, you must ensure it is reasonable and proportionate. You must ensure individuals know what is happening to their data unless an exemption or exception applies.

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

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

- In order to comply with the lawfulness principle you must identify a lawful basis for your data sharing and ensure your data sharing is lawful in a more general sense.

- Most data sharing, and the bulk of this code, is covered by the general processing provisions under Part 2 of the DPA; in practice this means referring to the GDPR. However data sharing by a "competent authority" for specific law enforcement purposes is subject to a different regime under Part 3 of the DPA for Law Enforcement Processing, which provides a separate but complementary framework.

- If a merger or acquisition or other change in organisational structure means that you have to transfer data to a different controller, you must take care. You must ensure you consider data sharing as part of your due diligence.

- The transfer of databases or lists of individuals is a form of data sharing. This may include sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies, and political parties. You are responsible for compliance with the law for the data you receive, and for data that is shared on your behalf. You must make appropriate enquiries and checks in respect of the data, including its source and any consent given.

- If you are considering sharing children's personal data, you must proceed with caution. You should consider the need to protect them from the outset. If the data sharing is of a type likely to result in a high risk to children's rights and freedoms, a DPIA is compulsory.

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

- 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 (the DEA). Data sharing under the DEA powers has to comply with the data protection legislation and with codes of practice that are consistent with this code.

- You should bear in mind ethical factors in addition to legal and technical considerations when deciding whether to share personal data. Data trusts are a relatively recent concept enabling independent third-party stewardship of data.

- 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 will always use our powers in a targeted and proportionate manner, in line with our regulatory action policy.

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 compliance with data protection legislation. It explains the law and provides good practice recommendations. Following it along with other ICO guidance will help you to: manage risks; meet high standards; clarify any misconceptions you may have; and give you confidence to share data appropriately and correctly.

In more detail

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):

> "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. 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 GDPR and the DPA.

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, the Commissioner must take the code into account when considering whether you have complied with your data protection obligations in relation to data sharing. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the GDPR or the DPA.

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

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 GDPR or the DPA.

If you process personal data in breach of this code and this results in a breach of the GDPR or the DPA, 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 €20 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 separate chapter on enforcement of this code.

What is the status of 'further reading' or other linked resources?

Any further reading or other resources which are mentioned in or linked from this code do not form part of the code. We provide links to give you helpful context and further guidance on specific issues, but there is no statutory obligation under the DPA for the Commissioner or the courts to take it into account (unless it is another separate statutory code of practice).

However, where we link to other ICO guidance, that guidance will inevitably reflect the Commissioner's views and inform our general approach to interpretation, compliance and enforcement.

Relevant provisions in the legislation

See DPA 2018 sections 121, 125 and 127

How should we use this code?

The code covers data sharing by organisations subject to the processing regimes under the GDPR and Part 2 of the DPA, and also the Law Enforcement (LE) regime in Part 3 of the DPA. Most data sharing is likely to be under the GDPR and Part 2 of the DPA, but where provisions differ we clarify this as far as possible. There is a separate chapter in this code on LE processing, that describes the differences in more detail, but controllers carrying out that type of processing should still read the whole of the code. The code does not cover data sharing under the Intelligence Services regime in Part 4 of the DPA.

The code is complementary to other ICO guidance and codes of practice relating to data protection. It assumes knowledge of key data protection terms and concepts. While the code stands alone as your guide to data sharing, it does not seek to reproduce other ICO guidance and you might need at times to refer out to guidance on the ICO website at www.ico.org.uk. This might be for an overview of data protection law or for more detailed guidance on

specific concepts, obligations and rights. 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 this 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.

Further reading outside this code

ICO's Guide to Data Protection
Guide to Law Enforcement Processing

Who is this code for?

The code is mainly aimed at organisations which are controllers sharing data subject to the GDPR and under the general data processing provisions of Part 2 of the DPA.

Controllers are defined under Article 4 of the GDPR. The code is also aimed at controllers sharing data under the Law Enforcement Processing (LE) regime (Part 3 DPA). There is a separate chapter for LE Part 3 data sharing. 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 third 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 the 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.

Relevant provisions in the legislation

See GDPR Articles 4(7) and 4(8)
See DPA 2018 section 3(9)

Further reading outside this code

Controllers and processors under the GDPR

What is the purpose of this code?

This code provides practical guidance for organisations about sharing personal data in compliance with data protection legislation. It explains the law and promotes good practice.

Many organisations using this code will have already shared data under the former data protection regime. This code should give you the knowledge and the confidence you need to continue sharing data under the GDPR and the DPA.

The code:

- updates and reflects key changes in data protection law since the last code was published (in particular from the GDPR and the DPA);
- explains new developments in technology 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.

Common concerns about data sharing

The code also clears up misconceptions about data sharing and barriers to sharing. The arrival of the GDPR and DPA in 2018 appears to have caused some concern amongst organisations about data sharing. However, 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.

For example:

Misconception
Data protection prevents us from sharing data.

Reality
Data protection does not prevent data sharing, as long as you approach it in a sensible and proportionate way. This code helps you to balance the risks and benefits and implement data sharing if it is:

- in the public interest; or
- proportionate, in the case of sharing for commercial reasons.

Misconception
The GDPR presents additional barriers to sharing data.

Reality
This is mistaken. Whilst the GDPR and DPA have changed some aspects of the law on data protection, they do not prevent you from data sharing. 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 under the new data protection legislation, even though there are some differences, which we explain in this code. Under the GDPR you must be certain you are accountable for your decision to share.

Misconception
There is little benefit to be gained from data sharing.

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

Misconception
We can only share data with people's consent.

Reality
Not always. You can usually share without consent if you have a good reason to do so. However, there are some cases where the impact on individuals might override your interests in sharing, in which case you might need to ask for their consent.

Misconception
We can't share data in an emergency.

Reality
You may be able to do so. And in an emergency scenario you should do whatever is necessary and proportionate. Please see our section on this topic later in the code.

The benefits of data sharing

The code also highlights the benefits that sharing personal data can bring to everyone: society, organisations, and individuals, whether as citizens or consumers. Data sharing, done in accordance with the law and good practice, can help government and other organisations deliver modern, efficient services and can make everyone's lives easier. Conversely, not sharing data can mean that everyone fails to benefit from these opportunities; and in some instances the chance is missed to assist citizens in need, whether in urgent or longer term situations.

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

- better compliance with the law;
- better protection for individuals whose data is being shared;
- greater trust in you by the public, 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; and
- a reduced reputational risk when sharing data.

Example

A local area set up an integrated care record to share patient records between health and social care staff. This 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 hospital emergency department and the local GPs introduced a data sharing process to enable the hospital's treating clinicians to have 24 hour secure access to the patient's GP record. The benefits of this arrangement included:

- better informed clinical decisions on how patients are treated based on previous medical history and current treatment plans;
- safer care by identifying current patient medications and allergies;
- a reduction in unnecessary emergency admissions and duplicate tests;
- removal of the burden on GPs having to print this information and provide it to the hospital; and
- improved patient experience and reduced service costs as clinicians and patients no longer had to wait for the information to arrive by other means.

Example

Several health professionals from different organisations 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 service users, they identified a pattern of evidence indicating that the person might be a victim of abuse. They shared this information with the person's social worker for further investigation.

Data sharing covered by this code

At a glance

This code covers the sharing of personal data between organisations which 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, data can be shared in an urgent or emergency situation.

In more detail

Data sharing covered by this 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 as "the disclosure of personal data by transmission, dissemination or otherwise making it available". This means giving personal data to a third party, by whatever means; and includes when you give a third party access to personal data on or via your IT systems.

For the purposes of this code, it does not include sharing data with employees, or with processors.

The following non-exhaustive list shows what data sharing could cover:

- a reciprocal or one-way exchange of data between organisations;
- an organisation providing another organisation with access to personal data on its IT system for a specific research purpose;

- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available 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 primary school passed details about a child showing signs of harm to the police or a social services department;
- the police passed information about the victim of a crime to a counselling charity;
- a retailer provided customer details to a payment processing company;
- the police and immigration authorities exchanged information about individuals thought to be involved in serious crime;
- a supermarket gave information about a customer's purchases to the police;
- a local authority disclosed personal data about its employees to an anti-fraud body;
- two neighbouring health authorities shared information about their employees for fraud prevention purposes;
- a school provided information about its pupils to a research organisation; and
- a multi-agency network group regularly exchanged information about individuals for safeguarding or social care purposes.

This code only applies to sharing 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 www.ico.org.uk if you need more information about anonymisation or pseudonymisation). Neither the GDPR, the DPA, nor this code of practice, applies to the sharing of information that does not constitute personal data.

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

- routine data sharing, sometimes known as "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 or unexpected or due to an urgent situation or 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 in a routine, pre-planned way. It will generally involve the sharing of data between organisations for an established purpose, perhaps the same sets of data, at regular, scheduled intervals.

A variation on this might be a group of organisations making an arrangement to share or pool their data for specific purposes, again on a 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

Sometimes organisations may decide, or are asked, to share data in situations which are not covered by any routine arrangement or agreement. It is still possible to share data in this type of scenario. 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 do what is necessary and proportionate.

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.

The organisations responsible for the data sharing would be regarded as joint controllers under Article 26 of the GDPR.

Data sharing between controllers

This code of practice 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 GDPR Article 4(7).

Sharing data with a processor

If a controller asks another party to process personal data on its behalf for the purposes of the GDPR the other party is a "processor", as defined in Article 4(8). The 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 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 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 under the GDPR. This type of arrangement is outside the scope of this code. For more details, you should refer to the guidance on the ICO website www.ico.org.uk.

Further reading outside this code

Contracts and liabilities between controllers and processors
Key definitions: controllers and processors
Guide to the GDPR: controllers and processors

Relevant provisions in the legislation

See GDPR Articles 4, 26 and 28 and Recitals 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 81 and 82 (external link)
See DPA 2018 section 121 (external link)

Deciding to share data

At a glance

When considering sharing data, you must consider your overall compliance with the data protection legislation. As a first step you should decide whether you need to carry out a Data Protection Impact Assessment (DPIA). We recommend you consider following the DPIA process, even where you are not legally obliged to carry one out.

In more detail

What do we need to do?

When considering sharing data, you must consider your overall compliance with the data protection legislation. As a first step, you should decide whether you need to carry out a Data Protection Impact Assessment (DPIA). You have to do this in order to demonstrate your compliance with the DPIA provisions. Even if you are not legally obliged to carry one out, we recommend you consider following the DPIA process.

Do we need to do a DPIA?

- You must do a DPIA for data sharing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.
- The GDPR gives examples of processing that require a DPIA:
    - where the use of innovative technology is likely to result in a high risk to the rights and freedoms of individuals;

    - automated decision-making (including profiling) resulting in a significant legal effect;
    - large-scale processing of special category data or criminal offence data; and
    - large-scale systematic monitoring of public spaces.

- It is also good practice to do a DPIA for any other major project which involves sharing personal data.
- In our view, examples of processing requiring a DPIA that might be relevant to data sharing also include:

    - data matching;
    - invisible processing; (there is more detail on this in the ICO's DPIA guidance); and
    - processing records where there is a risk of harm to individuals in the event of a data breach, such as whistleblowing or social care records.

There are instances other than the GDPR where a DPIA is obligatory; for example, pilots under the Digital Economy Act 2017.

In order to help you determine whether you need to carry out a DPIA you:

- can use our screening checklists on the ICO website; and
- should read the guidance on DPIAs on the ICO website www.ico.org.uk.

You should regard it as good practice to do a DPIA if you have any major project that involves the disclosure of 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 may not be legally required to do a DPIA. Nonetheless you can use the DPIA process as a flexible and scalable tool to suit your project.

What factors should we consider?

There are some practical and legal factors you should consider when you are deciding whether to share data.

This includes asking yourself the following questions:

- **What is the sharing meant to achieve?**
  When deciding whether to enter into an arrangement (whether one-off or ongoing and repeated) to share personal data (either as a provider, a recipient or both) you need to identify the objective(s) that the sharing is meant to achieve. You must have one or more clear objectives. This will allow you to work out what data you need to share and with whom. You must document this, and it would be good practice to do so in a data sharing agreement (also sometimes known as an information sharing agreement).

- **What information do we need to share?**
  You should only share the specific personal data needed to achieve your objectives. For instance, you might need to share somebody's current name and address, but not other information you hold about them.

- **Could we achieve the objective without sharing the data or by anonymising it?**
  If you can reasonably achieve the objective in another less intrusive way, you should not process the personal data. For example, where you could instead do this by sharing data that has been rendered anonymous (to which the GDPR doesn't apply) then you should do so, as it would be inappropriate to share the personal data itself in this context.

- **What risks does the data sharing pose to individuals?**
  Consider, for example, if any individual is likely to be harmed by it in any way, including physical, emotional, economic and social harms. Is any individual likely to object? Could it undermine individuals' trust in the organisations that keep records about them?

- **Is it right to share data in this way?**
  You should consider the potential benefits and risks, to both society and individuals, of sharing the data. Where appropriate, ethics should form a part of those considerations. Please also see the section on this later in the code. The proportionality of the data sharing exercise should be central to your analysis.

- **What would happen if we did not share the data?**

You should also assess the likely results of not sharing the data; this can itself be harmful.

- **Are we allowed to share the information?**
  Check whether there is any statutory bar or other restriction on sharing the data.

- **Who requires access to the shared personal data?**
  You should employ "need to know" principles, meaning that you should only share data to the extent that it is proportionate to do so:
  - other organisations should only have access to your data if they need it; and
  - only relevant staff within those organisations should have access to the data.

  As part of this, you should consider any necessary restrictions you may need to impose on the onward sharing of data with third parties.

- **When should we share it?**
  You must document this, for example whether the sharing should be an ongoing, routine process or whether it should only take place in response to particular events, and detail what these are.

- **How should we share it?**
  What are the processes for sharing the data? This must include security considerations and procedures around the transmission of data, and access to it by all those involved. For more on this, see later in the code.

- **How can we check the sharing is achieving its objectives?**
  You should refer to your objectives. What are you attempting to achieve by sharing this data? Being clear about this will help you measure whether the sharing has been successful. Then you can judge whether the data sharing is still appropriate, and whether the safeguards still match the risks.

- **Do we need to review the DPIA?**
  You must keep the risks of all data sharing arrangements under review, as with any form of data processing. If there is a significant change in the operation, such as the introduction of new technology, or a widening of scope, you should consider this as a trigger for a review of any existing DPIA (or PIA as it was formerly known), or for carrying out a

new assessment.

Sharing data outside the EEA

Will any of the data be transferred outside the European Economic Area (EEA)?

We will provide more guidance on this in due course. In the meantime you should refer to the guidance on the ICO website www.ico.org.uk for the latest position.

Relevant provisions in the legislation

See GDPR Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95
See DPA 2018 section 207 (external link)

Further reading outside this code

Data protection impact assessments
Detailed guidance on DPIAs
DPIA suggested template
DPIA checklists
International transfers
Data protection and Brexit

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB. The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Data sharing agreements

At a glance

It is good practice to have a data sharing agreement. It sets out the purpose of the data sharing, covers what is to happen to the data at each stage, sets standards and helps all the parties to be clear about their respective roles. It helps you to demonstrate your accountability under the GDPR.

In more detail

A data sharing agreement between the parties sharing and receiving data can form a major part of your compliance with the accountability principle of the GDPR. Sometimes a data sharing agreement is called an information sharing agreement, a data or information sharing protocol, or a personal information sharing agreement. It is good practice to have one in place.

What are the benefits of a data sharing agreement?

A data sharing agreement:

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

It should help you to justify your data sharing and to demonstrate that you have been mindful of, and have documented, the relevant compliance issues.

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 in question. Since a data sharing agreement is a set of common rules binding on all the

organisations involved in a data sharing initiative, you should draft the agreement in clear, concise language that is easy to understand.

Drafting and adhering to an agreement does not in itself provide you with any form of legal indemnity from action under the data protection legislation or other law. However The ICO will take this into account if it receives a complaint about your data sharing.

What should we include in a data sharing agreement?

In order to adopt good practice and to comply with the data protection legislation, the ICO expects you to address a range of questions in a data sharing agreement, including:

What is the purpose of the data sharing initiative?

Your agreement should explain:

- why the data sharing initiative is necessary;
- the specific aims you have; 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 identify clearly all the organisations that will be involved in the data sharing and should include contact details for their Data Protection Officer (DPO) and 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?

Where you are acting with another controller as joint controllers of personal data within the meaning of Article 26 of the GDPR, you are required to set out your responsibilities in an "arrangement". This may be done by means of a data sharing agreement. Under the transparency requirements of the GDPR you must make the essence of the agreement available to individual data

subjects. We recommend you do this in the privacy information you give to them.

What data items are we going to share?

Your agreement should explain the types of data you are intending to share with the organisations stated above. This may need to be quite detailed, because in some cases it will be appropriate to share only certain details 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 are allowed to access them, for example ones who have received appropriate training.

What is our lawful basis for sharing?

You need to explain clearly your lawful basis for sharing data. If you are a public sector organisation, you should also set out the legal power under which you are allowed to share it.

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

Is there any special category data or sensitive data?

You must document the relevant conditions for processing, as appropriate under the GDPR or the DPA, if the data you are sharing contains special category data or criminal offence data under the GDPR, or sensitive data within the meaning of Parts 2 or 3 of the DPA.

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. The agreement must make it clear 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, FOIA or the EIR. In particular, it should ensure that one staff member (generally a DPO) or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared data easily.

For joint controllers, Article 26 requires you to state in the agreement which controller is responsible for responding to individuals who exercise their data subject rights, although individuals may choose to contact any controller.

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

For public authorities, the agreement should also address the inclusion of certain types of information in your FOIA publication scheme.

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;
- are using compatible datasets and are recording data in the same way. The agreement could include examples showing how particular data items should be recorded, for example dates of birth;
- have common rules for the retention and deletion of shared data items 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;
- 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 provisions, for example relevant sections of the DPA, any legislation 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; 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
- decision form.

You can find examples of these in Annex B of this code.

When should we review a data sharing arrangement?

You should review your data sharing agreement on a regular basis because changes in circumstances or the rationale for the data sharing may arise at any point.

You should ask yourself the following key questions regularly:

- Is the data still needed? It's essential that you factor any new developments into your regular review of the data sharing arrangement to ensure that you can still justify the sharing. You may find you have achieved the aim of the data sharing and so no further sharing is necessary. On the other hand, you may find that the data sharing is making no impact upon your objective and therefore the sharing is no longer justified. If you cannot justify it, you should stop.
- Have you proactively communicated any changes to your data sharing arrangement to the people concerned?
- Do your privacy information and any data sharing agreements still explain the data sharing you are carrying out accurately?
- Are your information governance procedures still adequate and working in practice? All the organisations involved in the sharing should check whether:
    - it is necessary to share personal data at all, or you could use anonymised information instead;

    - you are only sharing the minimum amount of data and that the minimum number of organisations, and their staff members, have access to it;
    - the data you are sharing is still of appropriate quality;
    - all the organisations involved in the sharing are still applying the retention periods correctly;
    - all the organisations involved in the sharing have attained and are maintaining an appropriate level of security; and
    - staff are properly trained and are aware of their responsibilities for any shared data they have access to.
- Are you still providing people with all their individual rights under the GDPR or DPA as appropriate?
- Are you responding to people's queries and complaints properly and are you analysing them to make improvements to your data sharing arrangements?

Data protection principles

When sharing data, you must follow the key principles in data protection legislation. There are some differences between the principles in the respective pieces of legislation:

- Article 5 of the GDPR; and
- Sections 34-40 of Part 3 of the DPA for law enforcement processing.

We have reproduced the principles in Annex C to this code, and you should refer to the detailed guidance on the ICO website at www.ico.org.uk.

Further reading outside this code

Guide to the GDPR: principles
Guide to Law Enforcement processing

Accountability

At a glance

The accountability principle means that you are responsible for your compliance with the GDPR or DPA, as appropriate. You must be able to demonstrate that compliance by:

- maintaining documentation of all your data sharing operations;
- implementing appropriate security measures;
- recording any personal data breaches, and reporting them where necessary;
- carrying out data protection impact assessments (DPIAs) for any data sharing that is likely to result in high risk to the interests of individuals; and
- appointing a data protection officer (DPO) when appropriate.

You should review all your accountability measures regularly.

In more detail

What is the accountability principle?

Accountability is a legal requirement for data sharing; it is one of the principles applicable to general data processing under the GDPR, Part 2 of the DPA and law enforcement processing under Part 3.

The accountability principle requires that if you are involved in a data sharing arrangement you are responsible for your compliance with the GDPR or DPA as

appropriate, 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, adopting a "data protection by design and default" approach which will help you comply with the data protection legislation and good practice whenever you process data.

There is a general obligation to evidence your compliance and justify your approach, so you should adopt additional measures as necessary. A data sharing agreement would be one example of good practice to demonstrate your accountability. If you are unable to justify your approach, an accountability breach is likely, regardless of the outcome.

The importance of the accountability principle 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 all your employees.

What is data protection by design and default?

"Data protection by design and default" is a legal obligation requiring you to put in place appropriate technical and organisational measures to:

- implement the data protection principles in an effective manner; and
- safeguard individual rights.

This means that you have to hard-wire data protection throughout your data sharing processes, plans and activities.

There is more on technical measures relating to security in the chapter on security. Other technical measures include those designed to evidence compliance with other obligations. For example, technical measures that:

- give evidence of consent, including a timestamp as to information provided at the time; and
- ensure that withdrawals of consent, or objections, are processed properly and details are suppressed effectively.

What documentation do we need to keep?

Under Article 30 of the GDPR, larger organisations are required to maintain a record of their processing activities. Therefore you must ensure you document any data sharing you undertake, reviewing 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 GDPR, such as making sure that the information you hold and share about people is accurate and secure.

As well as your record of data sharing and other processing activities under Article 30, under Article 5(2) and Article 24 you also need to document other things to show your compliance with the GDPR. You need to keep sufficient documentation to be able to demonstrate your compliance with all principles, obligations and rights. As part of this, you must keep records of consent and of any personal data breaches.

You must document together all aspects of the data sharing, and other aspects of your compliance with the data protection legislation, such as your record of the lawful basis for processing and the privacy information you provide.

What is the role of the Data Protection Officer (DPO) in a data sharing arrangement?

If your organisation has a DPO, they should be closely involved from the outset in any plans to enter into a data sharing arrangement.

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 disclose or have received. Often the purpose of a data sharing arrangement involves very sensitive issues. 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.

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.

Shortly afterwards there were incidents of gang violence in the area and some victims had featured in the gangs database. Whilst it was not possible to establish a causal connection to the data breach, it was obvious that there would have been 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 to prevent such incidents happening, organisations processing sensitive data should have in place policies, processes and governance as well as training for staff. Conducting a data protection impact assessment (DPIA) is one way of helping an organisation to ensure it is complying with the law. This data sharing code also provides practical guidance.

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.

A call was taken by a new advisor late one evening by someone identifying themselves as a police officer and requesting the address of one of its clients. The organisation had protocols to follow about sharing data to third parties, and it was mandatory that all new advisors underwent this training on appointment. The advisor therefore knew the procedure to follow to determine whether or not they could share this information.

Relevant provisions in the legislation

See GDPR Articles 5(2), 25, 28,29,30,31,32,34,35, 38, 39 and Recitals 39, 81-83 (external link)
See DPA Part 3

Further reading outside this code of practice

ICO guidance on DPIAs, DPOs, documentation and accountability

Lawful basis for sharing personal data

At a glance

You must identify at least one lawful basis for sharing data from the start. You must be able to show that you considered this beforehand, in order to satisfy the accountability principle.

In more detail

What are the provisions on lawful basis?

You must identify at least one lawful basis for sharing data, from a number of provisions which are different for the GDPR and for Law Enforcement Processing under Part 3 of the DPA. This is known as a lawful basis for processing, and at least one must apply from the start of your data sharing. You must be able to show that you considered this before you started data sharing, in order to satisfy the accountability principle in the GDPR and Part 3 of the DPA. 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.

Lawful basis under the GDPR

For data sharing under the GDPR (and under Part 2 of the DPA), there are six lawful bases for processing, contained in Article 6. In summary they are as follows. For more details, you should refer to the ICO website at www.ico.org.uk.

(a) Consent: the individual has given their clear consent for you to share their personal data for a specific purpose.

(b) Contract: the sharing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the sharing is necessary for you to comply with the law (other than contractual obligations).

(d) Vital interests: the sharing is necessary to protect someone's life.

(e) Public task: the sharing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the sharing is necessary for your legitimate interests or those of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests, especially where the individual is a child. You cannot use legitimate interests as your lawful basis if you are a public authority processing data to perform your official tasks.

How do we determine which lawful basis is appropriate?

You should consider carefully all the background details to your plans for data sharing. Relevant factors include:

- the nature of the data;
- your purpose for sharing the data;
- the context of the sharing; and
- your relationship with the individual(s).

Most of the lawful bases in the GDPR require the processing to be "necessary" for a specific purpose. This assessment links to the DPIA process, which requires you to consider both necessity and proportionality. Ask yourself:

- do your plans help to achieve your purpose?
- is there any other reasonable way to achieve the same result?

"Necessary" means that the data sharing must be more than just useful, or standard practice. It must be a targeted and proportionate approach that is objectively necessary to achieve your stated specific purpose. If you can reasonably achieve the purpose by some other less intrusive means, or by sharing less information, you won't have a lawful basis for the data sharing and you should not go ahead.

You should decide which lawful basis applies before you start processing any personal data. It's important to choose the appropriate lawful basis from the start. You should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.

You must tell individuals about your lawful basis for sharing their data in your privacy notice, along with the other details you have to provide. Please see later in the code for details about privacy information.

For more information on how to determine which lawful basis is suitable for the data sharing you have in mind, please refer to the guidance on the ICO website at www.ico.org.uk.

What do we need to do if we are relying on legitimate interests as our lawful basis?

If you are relying on legitimate interests as your lawful basis for disclosing data to a third party, you must carry out a three-part test known as a legitimate interests assessment (LIA). This test considers some of the same questions as a DPIA, considering the necessity of the data sharing as well as individual rights. There is more information on this on the ICO website at www.ico.org.uk.

What do we need to do in respect of special category data and criminal offence data?

Some data sharing arrangements involve special category data. If you are sharing special category data under the GDPR, you must identify both a lawful basis for the sharing and an additional condition for doing so. Article 9(1) prohibits the processing of special category data but Article 9(2) lists conditions allowing its processing in certain circumstances. Some of the conditions listed in Article 9(2) are subject to conditions in Part 1 of Schedule 1 of the DPA. In summary these are around the following areas:

- employment;

- social security and social protection;
- health and social care;
- public health; and
- archiving, research and statistics.

If the data you plan to share concerns criminal convictions, criminal offences or related security measures, under Article 10 of the GDPR you must identify a lawful basis for general processing and either have "official authority" or meet a separate condition for processing this data under Schedule 1 of the DPA.

How do we determine which lawful basis is appropriate under Part 3 of the DPA - Law Enforcement Processing?

For data sharing carried out under the Law Enforcement provisions, it is only lawful "if and to the extent that it is based on law" and either:

- the individual has consented to the data sharing for that purpose; or
- the data sharing is necessary for the performance of a task carried out for that purpose by a competent authority.

What do we need to do about sensitive processing under Part 3 of the DPA?

For law enforcement processing the term "sensitive processing" is similar to special category data. If you want to share any data that falls under this heading, you must meet the requirements of one of the two cases set out in section 35 of Part 3 of the DPA:

<u>The first case</u>

- specific consent by the data subject to that data sharing for the law enforcement purpose in question; and
- when the sharing is carried out, you must have an "appropriate policy document" as defined in section 42.

<u>The second case</u>

- the processing is strictly necessary for law enforcement purposes;
- the processing meets at least one Schedule 8 condition; and

- when the sharing is carried out, you have an appropriate policy document.

Relevant provisions in the legislation

See GDPR Articles 6(1)(c), 6(1)(e), 6(1)(f), 6(3), 9(2), 13(1)(c), 14(1)(c), and Recitals 39, 41, 45, 47-49, 50, 51
See DPA 2018 sections 7, 8, 10, 11, 35, 42 and Schedules 1 (paras 6 and 7) and 8.

Further reading outside this code of practice

Lawful basis for processing
Lawful basis interactive guidance tool
Legitimate interests
Legitimate interests assessment
Guide to law enforcement processing

Fairness and transparency in data sharing

At a glance

You must always 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 also ensure that the sharing happens in a way that people would not find unexpected or objectionable, unless there is a good reason.
- You must ensure that individuals know what is happening to their data. They must know which organisations are sharing their personal data and which ones have access to that information, unless an exemption or exception applies.
- 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.

In more detail

Fairness and transparency are central to the data processing principles in the GDPR. You must always process personal data fairly and in a transparent manner.

Fairness also forms a key part of the principles under the Law Enforcement provisions of Part 3 of the DPA. Transparency is provided for in section 44 of the DPA for Part 3 processing.

How do we comply with the fairness principle when sharing data?

This principle applies to general processing under the GDPR and to processing under Part 3 of the DPA.

- 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 also ensure that the sharing happens in a way that people would not find unexpected or objectionable, unless there is a good reason. This is the case unless you are sharing due to a legal obligation or the sharing is necessary for law enforcement; the data sharing will take place despite any such concerns.
- You must comply with the fairness principle regardless of the type of sharing: whether you are sharing data on a routine basis or making a single one-off disclosure.
- You must meet the fairness requirement in data sharing in addition to demonstrating that you have a lawful basis for it. If any aspect of your processing is unfair, you will be in breach of the fairness principle – even if you can show that you have a lawful basis for the processing.
- You must treat fairly all the members of a group of individuals whose data you are sharing. If you treat most individuals fairly in your data sharing arrangement but treat even one individual unfairly, it will still be a breach of this principle.

Finally, sometimes data processing may take place in a way that negatively affects an individual but without this necessarily being unfair. The key here is whether the detriment is justified.

How do we assess whether we are sharing information fairly?

Some questions to consider:

- Is what you intend to do fair? Your planning process for the data sharing - including the steps as part of the DPIA (whether or not you are required to complete a DPIA) will help you to assess this.
- Should you share the personal data? Consider this, as well as thinking about how you can share the personal data.

- How did you obtain the data? For example, was anyone deceived or misled when you obtained the personal data? If so, using it for data sharing is unlikely to be fair.
- How does the data sharing affect the interests of the people whose data it is in general terms?

How do we comply with the transparency requirements when sharing data?

Individuals have to know what is happening to their data. The transparency principles under the GDPR and in section 44 in Part 3 of the DPA mean that you must ensure that individuals know which organisations are sharing their personal data and which ones have access to that information, unless an exemption or exception applies.

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. You must use clear and plain language that is suitable for your audience.

What privacy information do we need to provide under the GDPR?

When you collect personal data from individuals, under Article 13 of the GDPR you must provide them with privacy information which sets out what you intend to do regarding the collection and use of their data, and who else will be involved, including recipients or categories of recipients. Doing this is part of your compliance with your transparency obligations, where appropriate, and also fairness.

When you collect personal data from a third party, under Article 14 you must provide that information to individuals within a reasonable period and at the latest within a month. In a data sharing context this could be controllers sharing and receiving the data. You must provide the individual with the information "at the latest" when you first disclose the data to another recipient.

There are different methods of providing privacy information to individuals. You can provide privacy information using one or more techniques, but you must:

- include certain specific content;
- keep it up to date and proactively issue new information if you change the purpose of your data sharing or commence new data sharing; and
- give the information directly to individuals.

For more details, please see the guidance on the ICO website at www.ico.org.uk

Relevant provisions in the legislation

See GDPR Articles 5(1)(a), 13, 14 and Recitals 39, 58, 60-62 (external link)
See DPA 2018 Part 3 section 44 (external link)

Further reading outside this code of practice

ICO guidance on the right to be informed.
ICO guidance on the first principle

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 state of the art and costs of implementation when determining what measures are appropriate for your circumstances.

In more detail

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 chapter applies to processing under the GDPR and Part 3 of the DPA. These refer to security measures in relation to data processing in different ways:

- The security principle in the GDPR requires you to use "appropriate security"…"using appropriate technical or organisational measures ('integrity and confidentiality') and goes on to say more in Article 32.
- For Law Enforcement Processing under Part 3 of the DPA, you must use "appropriate technical or organisational measures" to ensure appropriate security of personal data.

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

What are the security considerations when sharing data?

You should consider the following measures for information that you share with other organisations, or that they share with you:

- review the personal data that you receive from other organisations. Make sure you know its origin and whether any conditions are attached to its use;
- review the personal data that you share with other organisations. Make sure you know who has access to it and what they will use it for;
- make sure you provide a suitably high level of security when sharing special category or sensitive data;
- identify who within your organisation should have access to data that has been shared with you. Adopt "need to know" principles and avoid giving all your staff access to the data when only a few of them need it to carry out their job;
- consider the impact a personal data breach may have on individuals; and
- consider the impact a personal data breach could have on your organisation – in terms of cost, reputational damage or lack of trust from your customers or clients. For example, this can be particularly acute where individuals have provided you with their data, you share it with another organisation, and that recipient organisation fails to protect that data.

You should aim to build a culture of compliance and good practice throughout your organisation to help you to ensure you are sharing data securely. This must apply from Board level, through all employees and contractors. For example:

- it is essential that all your staff involved in data sharing understand the importance of protecting personal data; and
- you should check that the same applies across the organisations you are sharing data with.

Before sharing data, you should undertake an information risk analysis and document your conclusions. As part of the assessment, you should bear in mind the nature of the information you are sharing. For instance, is it special category or sensitive data? You should regularly test, assess and evaluate your security provision.

This must include the actual transmission of the data you are sharing, and the way the data will be handled afterwards. You should consider the measures that you need to put in place to secure the data.

However you must not forget all other aspects of security, both physical and technical. You need to ensure you know and regularly review your security measures, both physical and technical, in both your own office and, where appropriate, that of the organisation you are sharing the data with. Details matter, including who has access to the data, and what access controls are in place to all hardware and software. Remember to consider building and office security, and resilience in the case of an incident such as a power failure or a fire.

You should also have clear instructions about the security steps that need to be followed when sharing information by multiple methods, eg phone, fax, post, email, online or face to face.

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:

- 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
- you should 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 data sharing. Please refer to the section on DPIAs in the chapter on "Deciding to share data" in this code.

Relevant provisions in the legislation

See GDPR Articles 5(1)(f), 32, 35, and Recitals 39, 83 (external link)

See DPA sections 40 and 91

Further reading – ICO guidance

Read our guidance on security in the Guide to the GDPR for more information.

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 with ease. You should provide them with a single point of contact and have clear policies and procedures with the other organisations.
You must inform the other organisations about requests for erasure, rectification or the restriction of processing, unless it is impossible or disproportionate to do so.
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?

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 under the GDPR and under Part 3 of the DPA differ in some respects.

The GDPR gives individuals specific rights over their personal data. For general data processing under Part 2 of the DPA, 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.

This chapter 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 www.ico.org.uk for more details.

How do you allow individuals to exercise their information rights in a data sharing scenario?

- You must have policies and procedures that allow individuals to exercise their rights with ease.
- 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 GDPR.
- 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 is responsible for being 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.

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 GDPR, individuals have a right to request erasure, rectification of their data, or the restriction of processing of their data. As with other individual rights, you will make life easier for yourself 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 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 to, you must also inform the individual about those organisations.

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

From time to time individuals 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 do the following:

- have procedures to deal with any complaints and queries in a quick and helpful way;
- provide a single point of contact;
- analyse the comments 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;
- if the responses you receive when you inform people about your data sharing consist of a significant number of objections, negative comments or other expressions of concern, use this information to help you review the data sharing in question;
- consider whether the comments you receive might suggest you should reduce the amount of data you share, or share it with fewer organisations;
- pay particular attention to concerns raised, and 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 automated decision-making?

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

So individuals can exercise their rights, you must:

- provide them with information about the automated process and the risks it entails;
- send them a link to your privacy statement if you have obtained their personal data indirectly;
- explain how they can access details of the information you used to create their profile;
- tell those who provided you with their own personal data how they can object to profiling, including profiling for marketing purposes; and
- inform them, and have the relevant procedures in place, about their right to access the personal data input into the profiles so they can review and edit it for any accuracy issues.

In addition you must have checks for the profiling/automated decision-making systems in your data sharing, in order to protect any vulnerable groups (including children). You must ensure at all times that you only collect the minimum amount of data you need and have a clear retention policy for the profiles you create.

What do we need to do about solely automated processing subject to Article 22?

Article 22 of the GDPR gives individuals additional protective rights if your data sharing arrangement entails a solely automated decision-making process that has legal or similarly significant effects on them. For example, automated profiling, depending on the impact on individuals. You must carry out a DPIA where you assess under Article 35(3)(a) of the GDPR that your proposed data sharing, involving systematic and extensive profiling based on automated processing, will "produce legal effects concerning the natural person or will similarly affect the natural person".

You can only carry out this type of automated decision-making if the decision is:

- necessary for the entry into or performance of a contract with the individual;
- authorised by law (in this code, we are looking at specific UK legal provisions, eg for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

You must identify whether any elements of your data sharing arrangement fall under Article 22. If they do, you must:

- give information to individuals about the automated processing;
- introduce simple ways for them to request human intervention or challenge a decision; and
- carry out regular checks to make sure that your systems are working as intended.

What individual rights are provided by Part 3 of the DPA: Law Enforcement Processing?

- 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 GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. There are also exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights. There is more guidance on this on the ICO website at www.ico.org.uk

Example

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

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

The procedures should also be provided in privacy information and should also be contained in any data sharing agreement.

Relevant provisions in the legislation

See GDPR Articles 16-19 and 22
Part 3 of the DPA

Further reading outside this code of practice - ICO guidance

ICO guidance on the rights of data subjects
Individual rights under the Law Enforcement Processing provisions

Other legal requirements

At a glance

In addition to identifying a lawful basis for your data sharing, you must ensure that your data sharing is lawful in a more 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.

Most private and third 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 sector organisation you should check your constitutional documents, legal agreements or any other legal or regulatory requirements to make sure there are no restrictions that would prevent you from sharing personal data in a particular context.

In more detail

The code has considered the data sharing requirements of the data protection legislation. This chapter now looks at some other requirements. It 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 of doing so. In addition to identifying a lawful basis for your data sharing, you must ensure that your data sharing is lawful in a more 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.

You must not confuse the lawfulness principle with legal powers. There is a link, though - if you do not have the legal power to share data, you will be in breach of the lawfulness principle.

Do we have a legal power to share data?

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

- whether you have a general legal power to share information, for instance, under your constitution. This is likely to be more relevant to public sector organisations; and
- 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 third sector.

What are the legal powers in the public sector?

When deciding whether you may proceed with any data sharing initiative, you should identify the legislation that is relevant to you. Even if this does not mention data sharing explicitly - and usually it will not do so - it is likely to lead you to a clearer understanding of your legal position.

Most public sector organisations derive their powers entirely from statute - either from the Act of Parliament which set them up, or from other legislation regulating their activities. The exceptions are government departments headed by a Minister of the Crown (which have common law powers to share information).

The relevant legislation will probably define 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 in question 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 will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances.

- **Express statutory powers**
  Sometimes, a public body will have an express power to share information. An express power will often be designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways". For instance, specific gateways exist under the Digital Economy Act 2017 (the 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. Please see elsewhere in this code for more details.

- **Implied statutory powers**
  Often, the legislation 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 the 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 GDPR. This requires the power to be laid down by law - but this does not need to be an explicit statutory provision. 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 the particular disclosure or data sharing arrangement in question. 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 third sector organisations?

The legal framework that applies to private and third sector organisations differs from that for public sector organisations. Most private and third 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 sector organisation you should check your constitutional documents, legal agreements or any other legal or regulatory requirements to make sure 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 third sector organisations should pay attention to any industry-specific regulation or guidance 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 in so far 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 (the Convention). 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 the sharing of 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, about the disclosure or data sharing arrangement you are proposing.

Have you checked whether there are any legal prohibitions on data sharing?

Your ability to share information may be subject to a number of legal constraints outside the data protection legislation. There might be other considerations such as specific statutory 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 legislation.

Relevant provisions in the legislation

European Convention on Human Rights: Article 8

Further reading outside this code

Lawful basis for processing
Guide to Law Enforcement Processing

Law Enforcement Processing: Part 3 DPA

At a glance

Most data sharing, and hence the bulk of this code, is covered by the general processing provisions under Part 2 of the DPA; in practice this means referring to the GDPR. However data sharing by a "competent authority" for specific law enforcement purposes is subject to a different regime under Part 3 of the DPA for Law Enforcement Processing, which provides a separate but complementary framework. As a competent authority, it is very likely that you will also be processing personal data for general purposes under Part 2 of the DPA, eg for HR-related matters. In that instance, you should follow the general guidance for Part 2 / GDPR data sharing.

In more detail

There are often 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 legislation does not prevent appropriate data sharing when it is necessary to protect the public, to support ongoing community 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.

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 police containing details of young teenagers.

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, without prejudicing their investigation.

Most data sharing, and hence the bulk of this code, is covered by the general processing provisions under Part 2 of the DPA; in practice this means referring to the GDPR. However data sharing by a **competent authority** for specific **law enforcement purposes** is subject to a different regime under Part 3 of the DPA, which provides a separate but complementary framework.

What is a competent authority?

A competent authority means:

- a person specified in Schedule 7 of the DPA; 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. 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 as:

Quote

"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".

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 Part 2 of the DPA, rather than for law enforcement purposes. An example might be for HR-related matters. In that instance, you should follow the general data sharing guidance contained elsewhere in this code.

We are a competent authority: how do we share data?

If you are a competent authority, and the sharing is for law enforcement purposes, then Part 3 may provide a framework allowing you to share data.

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

In particular, there are only six 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.

How do we share data with a competent authority?

If you are an organisation that **does not** fall within the Part 3 definition of a competent authority, then you can still share data for law enforcement purposes with a competent authority, such as the police in compliance with the GDPR. However you must still have a lawful basis for the sharing and you are also likely to need a condition for disclosing the data under Schedule 1 of the DPA.

Requests for information made 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 in DPA schedule 2, paragraph 2(1) from some GDPR provisions. This includes transparency obligations and most individuals' rights, if the application of these provisions is likely to prejudice the prevention or detection of crime.

If you are not a competent authority and are disclosing data relating to criminal offences and convictions (including allegations) you must comply with Article 10 of the GDPR. In practice this means:

- you again 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: disclosures necessary for prevention or detection of unlawful acts; and
- if meeting the public interest requirement is a problem, paragraph 36 of Schedule 1 provides a fall-back condition permitting the disclosure of criminal offence data, providing that the disclosure is necessary for the purposes of preventing or detecting an unlawful act; and asking for the individual's consent would prejudice those purposes.

If the data you are sharing includes special category data (eg information about race, ethnic origin, religion or biometric data), a condition under Article 9 of the GDPR will need to apply together with a linked condition in Schedule 1 of the DPA in most cases (most likely Article 9(2)(g) together with Schedule 1 paragraph 10 of the DPA).You must be able to demonstrate that the data sharing is necessary for reasons of substantial public interest.

The DPA usually requires organisations to have an "appropriate policy document" to cover their processing under this condition. However, an organisation disclosing data to a competent authority 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 it wanted it (some competent authorities may use a standard form for this).

The shopkeeper was processing data under the GDPR. Assuming the shopkeeper had a lawful basis for the processing, she could rely on Schedule 1, paragraph 10 to process the CCTV data, and give the police a copy of the footage to help with the investigation.

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

How do we allow individuals to exercise their information rights in a data sharing scenario under Part 3?

There are differences in the availability of individual rights for law enforcement processing. Certain individual rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the DPA. 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 ICO guidance on law enforcement processing at www.ico.org.uk.

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

Part 3 of the DPA requires you, as controller, to demonstrate that you comply with the principles. You are accountable.

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.

Example

There is an example earlier in the code, in the chapter on accountability, about the inappropriate disclosure of unredacted information by a council from a police intelligence database on gangs.

The police's own use of the gangs database in such an example would also need to address key issues of data retention, security, excessive data collection and sharing to enable the gangs programme to be lawful.
The aim of the data sharing between police and public sector organisations such as the local council to counter gang culture is a valid public interest to pursue.

A fair approach to data sharing, which is transparent in its purpose and accountable to obligations under data protection law, will gain the trust of our communities that are most directly affected, and so enhance the ability of community policing to engage with them.

You must also maintain relevant documentation of data processing activities. For more details, please refer to the ICO guidance on Law Enforcement Processing.

We have set out below the particular requirements of Part 3 documentation for data sharing.

Categories

When sharing data for law enforcement purposes, where relevant and as far as possible, you must make a clear distinction between different categories of personal data. You must distinguish between people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;

- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

Internal records of processing activities

Under Part 3 you must maintain detailed records of all data processing activities you undertake. This is a legal obligation. Your records must include the sort of details you would expect, such as:

- the purposes of your processing (this obviously includes any data sharing arrangements);
- categories of organisations with which you share personal data;
- the name of your DPO; and
- your security measures.

Logging

The following is likely to apply to many competent authorities that carry out data sharing. If your organisation operates any IT database for data processing, under Part 3 you must keep logs for specific processing operations such as collection, alteration, erasure and disclosures (including transfers). For more details, please refer to the ICO guidance on Law Enforcement Processing.

Relevant provisions in the legislation

See GDPR Articles 6, 9, 10 and Recitals 40, 41, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56 (external link)

See DPA 2018 sections 10, 11(2), 15, 30(1)(b), 31 and schedule 1 (paragraphs 10 and 36), 2 (paragraph 2) and 7 (external link)

Further reading outside this code of practice

Guide to Law Enforcement Processing
Guide to data protection

Due diligence when sharing data following mergers and acquisitions

At a glance

If merger or acquisition or other change in organisational structure means that you have to transfer data to a different or additional controller, you must take care. You must ensure you consider data sharing as part of the due diligence you carry out, including establishing the purposes for which the data was originally obtained, and your lawful basis for sharing it. You must comply with the principles, and document your data sharing. Consider when and how you will inform individuals about what's happening to their data. You must also ensure sound governance, accountability and security.

In more detail

This chapter 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, 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. We will look at this from the point of view of the organisation sharing the data with a different controller:

- ensure that you consider the data sharing as part of the due diligence you carry out;
- follow the data sharing guidance contained in this 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 individuals about what is happening. Under the 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 at www.ico.org.uk.

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 GDPR. You must:

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

Relevant provisions in the legislation

See GDPR Articles 5, 6, 7 and 21 and Recitals 39, 40, 42, 43, 50, 69, 70

Further reading outside this code

Guidance on individual rights under the GDPR

Sharing personal data in databases and lists

At a glance

The transfer of databases or lists of individuals, whether for money or other consideration, and whether for profit or not, is a form of data sharing. This may include sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies, and political parties.

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 will have to respond to any complaints about it. You should make appropriate enquiries and checks, including:

- confirm the source of the data;
- identify the lawful basis on which it was obtained;
- 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 relevant;
- 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 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.

In more detail

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

The transfer of databases or lists of individuals, whether for money or other consideration, and whether for profit or not, is a form of data sharing. This chapter 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;
- individual parts of a business that operate independently from their head office;
- clubs and societies;
- charities; and
- political parties.

The data protection legislation allows you to do this, so long as you comply with the law. You will also find it beneficial to follow the good practice set out in this code. The due diligence carried out by both the sharing and recipient controller 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 will 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;
- 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 relevant;
- 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 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.

You should consider having a written contract with the organisation supplying you with the data.

What else do we need to do?

Under Article 14 of the GDPR you must give privacy information to individuals whose data has been shared with you "…within a reasonable period after obtaining the personal data, but at the latest within one month…".

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. We will be issuing an updated direct marketing code of practice; you should refer to the ICO website at www.ico.org.uk.

How does data sharing interact with political campaigning?

Political parties, referendum campaigners and candidates use information about voters to help to target their campaign materials more effectively; they may:

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

This involves data sharing; and communicating with voters, such as via social media platforms and targeting political messages, may amount to direct marketing.

You should carry out the checks described earlier in this chapter 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 are sharing data with that external organisation. You should apply diligence in checking and monitoring what the third party is doing. You are responsible as controller for that data and for compliance with the legislation. You should read and follow the ICO guidance on the law relating to political campaigning and direct marketing on the website at www.ico.org.uk

Relevant provisions in the legislation

See GDPR Articles 13 and 14

Further reading outside the code of practice – ICO guidance

See the Direct marketing code and guidance on the ICO website in due course www.ico.org.uk

See the new Political campaigning guidance soon to be published on the ICO website 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 proceed with caution. You must consider the best interests of the child. You should consider the need to protect them from the outset.

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

We recommend that you do a DPIA to assess the risks involved in sharing this data. Sharing children's data with third parties can expose them to risks. If the data sharing is of a type likely to result in a high risk to children's rights and freedoms, a DPIA is compulsory.

In more detail

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

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

- You need to consider the best interests of the child. 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.
- 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 principle.

- Fairness, and compliance with the data protection principles, should be central to all the sharing you carry out of children's personal data. 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.
- 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 will not be compliant.
- You should not share personal data unless 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. Whereas selling on children's personal data for commercial re-use is unlikely to amount to a compelling reason for data sharing.
- 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 then you also need to comply with the Age-appropriate design code.

There is more information on all the above on the ICO website www.ico.org.uk

Relevant provisions in the legislation

See GDPR Articles 6(1), 8, 12(1) and Recitals 38, 58, 65, 71, 75

Further reading outside the code of practice

Guide to data protection: children
Children and the GDPR

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. If you are likely to be involved in responding to emergency situations it will be helpful to plan ahead as far as possible, by considering the types of data you hold and which data you are likely to need to share in advance.

In more detail

Much of the guidance in 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 emergency?

Urgent or emergency situations can arise that you may not have envisaged, and have to be dealt with on the spot. In an emergency you should go ahead and share data as is necessary and proportionate.

Tragedies over recent years such as the Grenfell Tower fire, and major terrorist attacks in London and Manchester, have illustrated the need for joined-up public services where data sharing can make a real difference to public safety. In these situations it would be more harmful not to share the data than to share it. You should factor in the risks involved in not sharing data.

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

In an emergency situation, you have to take decisions rapidly. Often, forward planning will help. Emergency services plan for various scenarios, and in the same way you should plan ahead for your organisation. In urgent or emergency situations, where 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 to share information during both the planning and recovery phases, where the need to share information may not be as urgent.

The key point is that the DPA does not prevent organisations sharing personal data where it is appropriate to do so. Factoring in the risks involved in not sharing data is particularly relevant in this situation.

Where possible, if you are likely to be involved in responding to emergency 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. All this should help you to establish what relevant data you hold, and help to prevent any delays in an emergency.

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.

Example

The police, the fire service and local councils get together to plan for identifying and assisting vulnerable people in their area in an emergency situation such as a flood, a major fire or a terrorist incident. As part of the process they determine what type of personal data they each hold and have a data sharing agreement to set out what they will share and how they will share it in the event of an emergency.

They review this plan at regular scheduled intervals.

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

At a glance

The government has devised a framework for the sharing of personal data, for defined purposes across specific parts of the public sector, under the Digital Economy Act 2017 (the DEA). The aim is to improve public services through the better use of data, while ensuring privacy, and to ensure clarity and consistency in how the public sector shares data. The DEA codes, which are required to be consistent with this data sharing code, provide guidance on the proportionate exercise of the tightly-defined DEA data sharing powers, in compliance with the data protection legislation.

The government introduced a framework for the sharing of personal data for defined purposes across specific parts of the public sector, under the Digital Economy Act 2017 (the DEA): the DEA framework. (Note that the DEA framework is distinct from the Framework for Data Processing by Government in section 191 of the DPA).

Its aim is to ensure clarity and consistency in how the public sector shares personal data, improving public services through the better use of data, while ensuring data privacy. The government also made it clear that data should only be shared 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 personal data with each other, in order to improve the delivery of public services. The objectives and purposes for data sharing under the DEA powers are tightly defined.

The organisations 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 be in compliance with the data protection legislation; and
- prohibits the disclosure of information where it would contravene the data protection legislation.

Note that whilst the DEA predates the GDPR, it was drafted with a view to being consistent with GDPR provisions.

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 codes must follow the data protection principles, ensuring that the sharing of personal data under the DEA powers is proportionate.

For example, there is a DEA code for public authorities sharing personal data information about the following aspects of public service delivery to:

- achieve specified public service delivery objectives;
- assist people living in fuel poverty and water poverty; and
- manage debt and 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, and data sharing for research purposes.

The DEA codes contain guidance as to what data you can share and for which purpose. They include safeguards to make sure that the privacy of citizens' data is protected. Public authorities have to put in place a data sharing agreement, described in the DEA codes as an "information sharing agreement".

Anyone who discloses information under the DEA Part 5 powers must also "have regard" to other codes of practice issued by the Information Commissioner "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
- the information to be provided to individuals about the use to be made of information collected from them.

More information will follow on the ICO website www.ico.org.uk about the DEA data sharing framework.

Relevant provisions in the legislation

Digital Economy Act 2017

Further reading outside this code

Digital Economy Act Part 5 Codes of practice

Data ethics and data trusts

At a glance

You should bear in mind ethical factors in addition to legal and technical considerations when deciding whether to share personal data.

Data trusts are a relatively recent concept: a legal structure that enables independent third-party stewardship of data. Pilot projects have taken place to demonstrate their use in data sharing.

In more detail

What is a data trust?

There is a great deal of interest, both in the UK and internationally, in the concept of 'data trusts'. There are various definitions of data trusts. The Open Data Institute (ODI) defines them as "a legal structure that provides independent third-party stewardship of data". In essence they are a new model to enable access to data by new technologies (such as artificial intelligence), while protecting other interests and retaining trust, and following a "privacy by design" approach. They have potential for use in data sharing.

What has been happening in the area of data trusts?

In 2019 the UK government announced that the ODI would be working with others on pilot projects to examine how a data trust could increase access to

data while retaining trust. It was also announced that in due course the ODI would make proposals as to the future use of data trusts.

The ICO will publish more information on data trusts in the future; please see the ICO website at www.ico.org.uk.

Is it ethical to share this data?

When deciding whether to enter into a data sharing arrangement, you should consider how that sharing would affect the individual's information rights, from an ethical stance.

Ask yourself whether it is:

- right to share that data in that particular way;
- the action of a responsible organisation;
- properly justified; and
- subject to clear and strong safeguards?

Data protection principles are based on respect for the fundamental rights of individuals. This is reflected in the requirements of the data protection legislation for fairness, transparency and accountability when processing personal data. Broadly speaking, ethical principles form a part of considerations on proportionality and fairness and are complementary to data protection principles. You should consider them in addition to considering the lawfulness and the technical requirements of data sharing.

What else should we consider?

You should also consider:

- any imbalance of power. There is a significant imbalance of power between organisations and individuals, and in particular vulnerable individuals. As an organisation you should act responsibly towards the needs not only of wider society but also of the individual; and
- the impact the data sharing would have on individuals' information rights regarding issues such as social exclusion, as well as on matters of equality and fundamental human rights. These might be the very matters you are intending to help to address in your data sharing plans,

so you need to give this careful thought, as you might need to strike a delicate balance.

What has been happening in the area of data ethics?

The UK government has taken an interest in data ethics.

In 2017 it announced the establishment of the Centre for Data Ethics and Innovation (CDEI) to investigate and advise on the use of data and data-enabled technologies and artificial intelligence, both in the public and private sectors.

In 2018 it published a Data Ethics Framework setting out clear standards for how data should be used in the public sector, with the aim of building confidence in public sector data use.

In 2015, the UK Statistics Authority (UKSA) established the National Statistician's Data Ethics Advisory Committee to provide independent and transparent advice to the National Statistician that the collection, access, use and sharing of data, for research and statistical purposes, is ethical and for the public good. The UKSA has also developed a self-assessment toolkit to provide guidance and support to researchers on how to assess and mitigate ethical risks in the context of their research.

Further reading outside this code of practice

Open Data Institute website
ODI article on data trusts
Government data ethics framework
Centre for Data Ethics and Innovation website
The National Statistician's Data Ethics Advisory Committee

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 where appropriate. This includes the power to issue warnings, reprimands, stop-now orders and fines. 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?

The Information Commissioner 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.

We have also introduced initiatives such as the Sandbox to help 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 will the ICO monitor compliance?

We will 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 with a view to guaranteeing 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 GDPR or DPA, 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. However, 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 individuals 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 DPA, we have the power to take enforcement action. This may require you to take steps to bring your operations into compliance or we may decide to fine you or both.

What are the ICO's enforcement powers?

We have various powers to take action for a breach of the GDPR or DPA. We have a statutory duty to take the provisions of this code into account when enforcing the GDPR and DPA.

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 €20 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 business is able to operate and innovate efficiently in the digital age. We will be as robust as we need to be in upholding the law, whilst ensuring that commercial enterprise is not constrained by red tape, or concern that sanctions will be used disproportionately.

These powers are set out in detail on the ICO website at www.ico.org.uk.

Relevant provisions in the legislation

See GDPR Articles 12-22 and Recitals 58-72 (external link)
See DPA 2018 section 129-164 and schedule 12 (external link)

Further reading outside this code

What we do
Make a complaint
Regulatory Action Policy
Guide to the ICO Sandbox - beta phase

Annex A: data sharing checklists

These will be added before the final publication stage.

Annex B: template data sharing request and decision forms

These will be added before the final publication stage.

Annex C: data protection principles

The data protection principles for the general processing of data (ie under part 2 of the DPA) are those stated in the GDPR. However there are some differences in the principles applicable to Law Enforcement Processing under Part 3 and Intelligence Services Processing under Part 4.

For your ease of reference, we have reproduced each of them below. You should also refer to the ICO's guidance at www.ico.org.uk

- GDPR data protection principles
- Data Protection Act 2018 Part 3: Principles applicable to Law Enforcement Processing

GDPR data protection principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data

are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Data Protection Act 2018 Part 3: Principles applicable to Law Enforcement Processing

34 Overview and general duty of controller

(1) This Chapter sets out the six data protection principles as follows—

(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and

(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.

(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.

35 The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(6) The Secretary of State may by regulations amend Schedule 8—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(7) Regulations under subsection (6) are subject to the affirmative resolution procedure.

(8) In this section, "sensitive processing" means—

(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;

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

36 The second data protection principle

(1) The second data protection principle is that—

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that—

(a) the controller is authorised by law to process the data for the other purpose, and

(b) the processing is necessary and proportionate to that other purpose.

(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

37 The third data protection principle

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

38 The fourth data protection principle

(1) The fourth data protection principle is that—

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as—

(a) persons suspected of having committed or being about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) persons who are or may be victims of a criminal offence;

(d) witnesses or other persons with information about offences.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose—

(a) the quality of personal data must be verified before it is transmitted or made available,

(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and

(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

39 The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

40 The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Annex D: case studies

Fairness and transparency

Supermarket providing privacy information to customers

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

The supermarket or the card scheme operator should have given 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 discloses information about a particular scheme member to the police, it does not need to inform the individual of the disclosure if this would prejudice crime prevention.

Fairness and transparency

Sharing customer details with a credit reference agency

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

It must inform customers when they open an account that it will 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 must ensure it is collecting adequate information to distinguish between individuals, for example dates of birth.

The organisations involved must have procedures to deal with complaints about the accuracy of the information they have shared.

Fairness and transparency; privacy information

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

Personal information is shared between two county councils and 19 relevant partner organisations in order to prevent social exclusion amongst young people who have been, or are at high risk of disengaging from education, employment or training. By sharing information the partner organisations can ensure a co-ordinated approach to identifying and contacting each young person to offer the most appropriate support to encourage them back in to education, work or training.

As part of developing their data sharing agreement, all the partners updated their privacy notices to include this new data sharing and agreed that each organisation would communicate this via their websites as well as in correspondence and conversations their staff have with the young people.

Fairness and transparency

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

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

The DPA 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, may be inferred from the Pupil Premium status of a child. Parents and their children may well object to the disclosure of this data because they consider it sensitive and potentially stigmatising. Data about a child's academic performance could be considered equally sensitive.

Instead the school could identify eligible children on the researchers' behalf and contact their parents, explaining what the research is about, what data the researchers want. The school might wish to obtain parents' consent for the sharing of the data, but other lawful bases would be available to it.

Alternatively, the school could disclose 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 legislation 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 have to tell their story once and can expect a better service delivery;
- local people have clear guidance about how their information is shared (and in what circumstances their consent may need to be sought to share it);
- professionals have access to the information they need, when they need it, to support better outcomes for local people;
- good decision making is supported by an information sharing framework providing staff with clear direction; and
- unnecessary appointments and admissions can 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 will 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 need to be empowered to feel confident about sharing information between partners. Senior leaders need to be visible to give staff the confidence to share patient information.
- Internal culture needs to be supportive. The culture needs to be underpinned by strong values and ethos. It is essential that a learning culture is developed so that mistakes can be shared and learnt from rather than brushed aside. This learning includes developing formal training for all staff who were using an integrated care record, supported by the framework.
- Transparency needs to be established so that there is a collective understanding of how the data will be shared and by whom it will be shared. Staff need to have clarity around their roles and responsibilities and the benefits of sharing information.
- Need to develop a culture of appropriate sharing in plain English. Messages need to be simplified to avoid confusion and jargon needs to be reduced.

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

Data sharing required by law

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

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

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

There is no point in the local authority seeking employees' consent for the sharing because the law says the sharing can take place without consent. The local authority should also be clear with its employees that even if they object to the sharing, it will still take place.

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

Lawful basis; special category data; fairness and transparency; accountability

Considerations in relation to a healthcare data sharing agreement

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

The partner organisations have developed a data sharing agreement to support their joint mental health policy. Depending on the circumstances of each case, the lawful basis may be consent or a task carried out in the public

interest. The data sharing agreement clearly identifies the various pieces of legislation that each partner relies on to specify their public functions and the provisions they need to meet if relying on consent. As special category data is likely to be necessary for referrals, they have also identified Article 9 conditions. The data sharing agreement reminds all parties to maintain the rights and dignity of patients, their carers and families, involving them in risk assessments wherever possible whilst also ensuring their safety and that of others.

Data sharing agreement; accountability; information rights

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

Personal information is 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 have been, or are at high risk of, disengaging from education, employment or training. By sharing the information, the partner organisations can ensure a co-ordinated approach to providing the most appropriate support to the young person to encourage them back in to 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 related to 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 Companies House and lower figures at HMRC, they will simultaneously

increase their creditworthiness with financial institutions and wider government whilst also reducing tax liabilities.

Until 2018, restrictions on data sharing had prevented HMRC and Companies House 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, Companies House 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 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 Companies House in October 2018 – the very first transfer of data under the Digital Economy Act powers.

The pilot sought to address the fraud problem through ten 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 Companies House back office data to uncover previously hidden links between companies, combined for the first time with HMRC intelligence.

The data-sharing pilot identified £14.6m of savings, with a further £100.6m 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.