Data protection

Data sharing code of practice

ico.
Information Commissioner's Office

Contents

1 Information Commissioner's foreword

As I said in launching the public consultation on the draft of this code, under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors – both public and private. But citizens' and consumers' rights under the Data Protection Act must be respected. Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness. But when things go wrong this can cause serious harm. We want citizens and consumers to be able to benefit from the responsible sharing of information, confident that their personal data is being handled responsibly and securely.

Following the consultation, we've been able to take on board many helpful points made by our stakeholders. I am grateful to everyone who has helped to make this code as comprehensive and helpful as possible.

The code's title refers to 'data sharing'. That is to use the language of the new provisions of the Data Protection Act – and it's that legislation that requires me to produce this code. But the code isn't really about 'sharing' in the plain English sense. It's more about different types of disclosure, often involving many organisations and very complex information chains; chains that grow ever longer, crossing organisational and even national boundaries.

Information rights are higher than ever on the public agenda. That's because more and more transactions are done online – by us or about us. Shopping, entertainment, banking, communicating, socialising – but also tax, pensions, benefits, health records, council services and so on. That's not going to go away – in fact, it's only going to grow.

People want their personal data to work for them. They expect organisations to share their personal data where it's necessary to provide them with the services they want. They expect society to use its information resources to stop crime and fraud and to keep citizens safe and secure. However, people also want to know how their information is being used, who has access to it, and what that means for them. People also expect an appropriate level of choice and control, especially over their sensitive data.

This code of practice is inevitably written in general terms, providing a framework for organisations to make good quality decisions about data sharing. The code cannot provide detailed advice relevant to every situation in which data sharing takes place. If they have not done so already, organisations working in specialist areas – policing or credit referencing, for example – may need to produce their own detailed, bespoke data sharing guidance. This code of practice will help organisations to do this, and the ICO will provide whatever advice and assistance it can.

As the name suggests, this code is about 'practice' – about doing, about delivering information rights in the real world. Adopting its good practice recommendations will help organisations to work together to make the best use of the data they hold to deliver the highest quality of service, whilst avoiding the creation of the opaque, excessive and insecure information systems that can generate so much public distrust.

Christopher Graham
Information Commissioner

2 About the code

This code explains how the Data Protection Act 1998 (DPA) applies to the sharing of personal data. It also provides good practice advice that will be relevant to all organisations that share personal data.

The code covers activities such as:

- a group of retailers exchanging information about former employees who were dismissed for stealing;
- a local authority disclosing personal data about its employees to an anti-fraud body;
- a primary school passing details about a child showing signs of harm to the police or a social services department;
- the police passing information about the victim of a crime to a counselling charity;
- a GP sending information about a patient to a local hospital;
- the police and immigration authorities exchanging information about individuals thought to be involved in serious crime;
- a supermarket giving information about a customer's purchases to the police;
- two departments of a local authority exchanging information to promote one of the authority's services;
- two neighbouring health authorities sharing information about their employees for fraud prevention purposes;
- a school providing information about pupils to a research organisation; and
- a retailer providing customer details to a payment processing company.

Who should use this code of practice?

Any data controller who is involved in the sharing of personal data should use this code to help them to understand how to adopt good practice. Much of the good practice advice will be applicable to public, private and third sector organisations. Some parts of the code are necessarily focused on sector-specific issues. However, the majority of the code will apply to all data sharing regardless of its scale and context.

How the code can help

Adopting the good practice recommendations in this code will help you 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 to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data when it is appropriate to do so, but should also give you a clearer idea of when it is not acceptable to share data.

Specific benefits of this code for organisations include:

- minimised risk of breaking the law and consequent enforcement action by the ICO or other regulators;
- better public trust by ensuring that legally required safeguards are in place and complied with;
- better protection for individuals when their data is shared;
- increased data sharing when this is necessary and beneficial;
- greater trust and a better relationship with the people whose information you want to share;
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or consent or in the face of objection; and
- reduced risk of questions, complaints and disputes about the way you share personal data.

The code's status

The Information Commissioner has prepared and published this code under section 52 of the Data Protection Act. It is a statutory code. This means it has been approved by the Secretary of State and laid before Parliament. The code does not impose additional legal obligations nor is it an authoritative statement of the law. However, the code can be used in evidence in any legal proceedings, not just proceedings under the DPA. In determining any question arising in proceedings, courts and tribunals must take into account any part of

the code that appears to them to be relevant to that question. In carrying out any of his functions under the DPA, the Information Commissioner must also take into account any part of the code that appears to him to be relevant to those functions.

This code is the ICO's interpretation of what the DPA requires when sharing personal data. It gives advice on good practice, but compliance with our recommendations is not mandatory where they go beyond the strict requirements of the Act. The code itself does not have the force of law, as it is the DPA that places legally enforceable obligations on organisations.

Organisations may find alternative ways of meeting the DPA's requirements and of adopting good practice. However, if they do nothing then they risk breaking the law. The ICO cannot take enforcement action over a failure to adopt good practice or to act on the recommendations set out in this code unless this in itself constitutes a breach of the DPA.

Although the DPA sets out the bare legal requirements to be considered when sharing personal data, it provides no guidance on the practical measures that could be taken to comply with them. This code helps to plug that gap.

3 What do we mean by 'data sharing'?

By 'data sharing' we mean the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

- a reciprocal exchange of data;
- 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;
- exceptional, one-off disclosures of data in unexpected or emergency situations; or
- different parts of the same organisation making data available to each other.

Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared. Neither the Data Protection Act (DPA), nor this code of practice, apply to that type of sharing.

The code covers the two main types of data sharing:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

Different approaches apply to these two types of data sharing and the code of practice reflects this. Some of the good practice recommendations that are relevant to systematic, routine data sharing are not applicable to one-off decisions about sharing.

'Systematic' data sharing

This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

Ad hoc or 'one-off' data sharing

Much data sharing takes place in a pre-planned and routine way. As such, it should be governed by established rules and procedures. However, organisations may also decide, or be asked, to share data in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

Sharing with a 'data processor'

This code of practice is mainly about sharing personal data between data controllers – i.e. where both organisations determine the purposes for which and the manner in which the personal data is processed.

However, there is a form of data sharing where a data controller shares data with another party that processes personal data on its behalf. In the DPA, these organisations are known as 'data processors'.

The DPA draws a distinction between one data controller sharing personal data with another, and a data controller sharing data with its data processor. The DPA requires that a data controller using a data processor must ensure, in a written contract, that:

- the processor only acts on instructions from the data controller; and
- it has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle.

Therefore a data processor involved in data sharing doesn't have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller.

Sharing within organisations

When we talk about 'data sharing' most people will understand this as sharing data between organisations. However, the data protection principles also apply to the sharing of information within an organisation – for example between the different departments of a local authority or financial services company. Whilst not all the advice in this code applies to sharing within organisations, much of it will, especially as the different parts of the same organisations can have very different approaches to data protection, depending on their culture and functions.

4 Data sharing and the law

Before sharing any personal data you hold, you will need to consider all the legal implications of doing so. Your ability to share information is subject to a number of legal constraints which go beyond the requirements of the Data Protection Act (DPA). There may well be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect your ability to share personal data. A duty of confidence may be stated, or it may be implied by the content of the information or because it was collected in circumstances where confidentiality is expected – medical or banking information, for example. You may need to seek your own legal advice on these issues.

If you wish to share information with another person, whether by way of a one-off disclosure or as part of a large-scale data sharing arrangement, you need to consider whether you have the legal power or ability to do so. This is likely to depend, in part, on the nature of the information in question – for example whether it is sensitive personal data. However, it also depends on who 'you' are, because your legal status also affects your ability to share information – in particular it depends on whether you are a public sector body or a private/third sector one.

The public sector

Most public sector organisations, other than government departments headed by a Minister of the Crown (which have common law powers to share information), derive their powers entirely from statute – either from the Act of Parliament which set them up or from other legislation regulating their activities. Your starting point in deciding whether any data sharing initiative may proceed should be to identify the legislation that is relevant to your organisation. Even if this does not mention data sharing explicitly, and usually it will not do so, it is likely to lead you to the answer to this question.

The relevant legislation will probably define the organisation's functions in terms of its purposes, the things that it must do, and the powers which the organisation may exercise in order to achieve those purposes, the things that it may do. So it is necessary to identify where the data sharing in question would fit, if at all, into the range of things that the organisation is able to do. Broadly speaking, there are three ways in which it may do so:

- **Express 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 but, where such an obligation applies, it is clearly permissible to share the information.

- **Express powers** – Sometimes, a public body will have an express power to share information. Again, 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".
- **Implied 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. To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be "reasonably incidental", and then check that the organisation has the power to engage in that activity.

Whatever the source of an organisation's power to share information, you must check that the power covers the particular disclosure or data sharing arrangement in question – otherwise, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. This might be the case where an NHS Trust breaches a duty of confidentiality because a doctor believes that a patient has been involved in serious crime. Whilst a disclosure in the public interest may be defensible in a particular case, this does not constitute a legal power to share data.

Private and third sector organisations

The legal framework that applies to private and third sector organisations differs from that which applies to public sector organisations, which may only act within their statutory powers. However, all bodies must comply fully with the data protection principles.

In some private sector contexts there are legal constraints on the disclosure of personal data. However, most private and third sector organisations have a general ability to share information provided this does not breach the DPA or any other law. It is advisable for a company to check its constitutional documents, such as its memorandum and articles of association, to make sure there are no restrictions that would prevent it from sharing personal data in a particular context.

Private and third sector organisations should have regard to any industry-specific regulation or guidance about handling individuals' information as this may affect the organisation's ability to share information. They should also be aware of the legal issues that can arise when sharing personal data with public sector bodies. This becomes more of an issue as private and third sector bodies are carrying out a wider range of traditionally public sector functions.

Human rights

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature. Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal data. Article 8 is not an absolute right – public authorities are permitted to interfere with it if it is lawful and proportionate to do so.

It is advisable to seek specialist advice if the disclosure or data sharing arrangement you are proposing engages Article 8 or any other Convention right. However, if you disclose or share personal data only in ways that comply with the DPA, the sharing or disclosure of that information is also likely to comply with the HRA.

5 Deciding to share personal data

Factors to consider

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you need to identify the objective that it is meant to achieve. You should consider the potential benefits and risks, either to individuals or society, of sharing the data. You should also assess the likely results of not sharing the data. You should ask yourself:

- **What is the sharing meant to achieve?** You should have a clear objective, or set of objectives. Being clear about this will allow you to work out what data you need to share and who with. It is good practice to document this.
- **What information needs to be shared?** You shouldn't share all the personal data you hold about someone if only certain data items are needed to achieve your objectives. For example, you might need to share somebody's current name and address but not other information you hold about them.
- **Who requires access to the shared personal data?** You should employ 'need to know' principles, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.
- **When should it be shared?** Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
- **How should it be shared?** This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
- **How can we check the sharing is achieving its objectives?** You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.
- **What risk does the data sharing pose?** For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?
- **Could the objective be achieved without sharing the data or by anonymising it?** It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- **Do I need to update my notification?** You need to ensure that the sharing is covered in your register entry.
- **Will any of the data be transferred outside of the European Economic Area (EEA)?** If so, you need to consider the requirements of the eighth principle of the Data Protection Act (DPA). For more detailed guidance on this area see: www.ico.gov.uk

Conditions for processing

The first data protection principle says that organisations have to satisfy one or more 'conditions' in order to legitimise their processing of personal data, unless an exemption applies. Organisations processing sensitive personal data, for example information about a person's health, will need to satisfy a further, more exacting condition. It is important to be clear that meeting a condition for processing will not in itself ensure that the sharing of personal data is fair or lawful. These issues need to be considered separately.

Consent (explicit consent for sensitive personal data) is one of the conditions the DPA provides to legitimise processing. The Data Protection Directive on which the UK's DPA is based defines 'the data subject's consent' as:

'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

There must therefore be some form of active communication where the individual knowingly indicates consent. Whilst consent will provide a basis on which organisations can share personal data, the ICO recognises that it is not always achievable or even desirable. If you are going to rely on consent as your condition you must be sure that individuals know precisely what data sharing they are consenting to and understand its implications for them. They must also have genuine control over whether or not the data sharing takes place. It is bad practice to offer individuals a 'choice' if the data sharing is going to take place regardless of their wishes, for example where it is required by statute or is necessary for the provision of an essential service.

Consent or explicit consent for data sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so;
- the individual would be likely to object should the data be shared without his or her consent; or
- the sharing is likely to have a significant impact on an individual or group of individuals.

The other conditions that provide a basis for processing non-sensitive personal data include:

- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

The 'legitimate interests' condition provides grounds to process personal data in a situation where an organisation needs to do so for the purpose of its own legitimate interests or the legitimate interests of the third party that the information is disclosed to. This condition cannot be satisfied if the processing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the individual whose data is being processed. This condition cannot legitimise the processing of sensitive personal data.

For example, a catalogue company providing extreme sports accessories wants to sell a list of customer names and addresses onto a travel agent that offers adventure holidays. In this case the legitimate interests condition is likely to be the catalogue company's basis to process this data. The data shared is not sensitive personal data and their use of the information in this scenario is unlikely to prejudice the rights and freedoms or legitimate interests of the customers. Having a condition for processing will not ensure that the processing will meet the other requirements of the DPA. The catalogue company needs to consider the fairness requirements of the Act and would need to comply with the other principles.

The conditions for processing sensitive personal data are more difficult to satisfy. For example if you want to process medical data you have to satisfy a condition from the list above and also a more stringent sensitive data condition – one of which specifically legitimises processing of health data for medical purposes, including the provision of treatment and medical research. For more details of all the conditions for processing and the circumstances in which they apply see the Guide to data protection: www.ico.gov.uk

6 Fairness and transparency

The Data Protection Act (DPA) requires that personal data be processed fairly. This means that people should generally be aware of which organisations are sharing their personal data and what it is being used for. In a broader sense, fairness also requires that where personal data is shared, this happens in a way that is reasonable and that people would be likely to expect and would not reasonably object to if given the chance. You need to think about this before you first share any personal data. This applies equally to routine data sharing or a single, one-off disclosure.

Privacy notices

The ICO has already produced comprehensive good practice guidance on the drafting and distribution of privacy notices – sometimes known as fair processing notices – in our Privacy notices code of practice. This is available at: www.ico.gov.uk

Much of the guidance on privacy notices is particularly relevant in data sharing contexts because of the need to ensure that people know which organisations are sharing their personal data and what it is being used for.

In a data sharing context, a privacy notice should at least tell the individual:

- who you are;
- why you are going to share personal data; and
- who you are going to share it with – this could be actual named organisations or types of organisation.

You should provide a privacy notice when you first collect a person's personal data. If you have already collected their personal data, then you need to provide them with the information above as soon as you decide that you're going to share their data or as soon as possible afterwards.

In some cases a single privacy notice will be enough to inform the public of all the data sharing that you carry out. This might be the case where personal data is being shared with a number of organisations for marketing purposes. However, if you are engaged in various significant data sharing activities, it is good practice to provide information about each one separately. This will allow you to give much more tailored information, and to target it at the individuals affected by the particular sharing. There is a danger that

individuals affected by data sharing will not be able to find the information they need if an organisation only publishes one all-encompassing privacy notice.

Data sharing arrangements can change over time – for example where a law is introduced that requires an organisation to take part in a new data sharing operation. As a result, it is good practice to review your privacy notice regularly so that it continues to reflect accurately the data sharing you are involved in. Any significant changes to your privacy notice need to be publicised appropriately – depending primarily on the impact of the changes on individuals.

Telling individuals about data sharing

The DPA leaves it open as to how, or whether, you have to provide a privacy notice. In some cases it is enough just to have a privacy notice available so people can access it if they want to. This approach is acceptable where the data sharing is something people are likely to expect or be aware of already, and to which people are unlikely to object.

For example, a user of an online retail site is aware through the nature of the transaction that the retail site will disclose certain information to a secure payment service and to a courier service in order to take payment for goods and arrange their delivery. Where this is already clear, there is no need to inform the individual actively that personal data is being shared.

In other cases it is good practice to communicate a privacy notice actively. This is a legal obligation where a failure to do so would result in unfairness to the individual. By 'communicate actively' we mean taking a positive action to provide a privacy notice, for example by sending a letter, reading out a script or distributing an email.

A good way to decide whether to communicate a notice actively is to try to anticipate whether the individual would expect their personal data to be shared or would object if they knew about it.

The need to communicate a privacy notice actively is strongest where:

- you are sharing sensitive personal data; or
- the data sharing is likely to be unexpected or objectionable; or
- sharing the data, or not sharing it, will have a significant effect on the individual; or
- the sharing is particularly widespread, involving organisations individuals might not expect; or
- the sharing is being carried out for a range of different purposes.

Who should tell the individual?

Data sharing typically involves personal data being disclosed between a number of organisations, all of whom have a responsibility to comply with the DPA, including its fairness provisions.

The most important thing is to ensure that the organisations involved in data sharing work together to ensure that the individuals concerned know who has, or will have, their data and what it is being used for, or will be used for. The primary responsibility for doing this falls to the organisation that collected the data initially. However, it is good practice for all the organisations involved to ensure that, throughout the data sharing process, individuals remain aware of who has their personal data and what it is being used for. This is particularly important where the data has been disclosed to another organisation or where it is being used for a different purpose. It is good practice for recipients of personal data to check the privacy notice of the organisation that collected the data originally, to check whether it describes the types of recipient and their use of the data.

Sharing without the individual's knowledge

The general rule in the DPA is that individuals should, at least, be aware that personal data about them has been, or is going to be, shared – even if their consent for the sharing is not needed. However, in certain limited circumstances the DPA provides for personal data, even sensitive data, to be shared without the individual even knowing about it.

You can share without an individual's knowledge in cases where, for example, personal data is processed for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty.

An organisation processing personal data for one of these purposes is exempt from the fairness requirements of the DPA, but only to the extent that applying these provisions would be likely to prejudice the crime and taxation purposes. For example, the police might ask an organisation to give them information about an ex-employee who they suspect of being involved in a serious assault. If informing the ex-employee that they have given the police this information would tip the individual off and be likely to prejudice the investigation, because the suspect might abscond for example, then the organisation could rely on the exemption and wouldn't have to tell the individual about the disclosure of information.

The exemptions are explained in our Guide to data protection: www.ico.gov.uk

In some cases the sharing of data is required by law, for example under the Money Laundering Regulations 2007 – these allow financial institutions to share personal data with law enforcement agencies in certain circumstances. Such legal requirements override an individual's consent or objection. However, it is still good practice, and may still be a legal obligation, to explain in general terms to all individuals the circumstances in which their personal data may be shared and the likely consequences of this.

It is also good practice to tell the individual as soon as you can after the risk of prejudice has passed that information about them has been shared. This will not be practicable where the organisation providing the information is unaware of the progress or outcome of an investigation. Secrecy may be maintained where this would be likely to prejudice future policing operations, for example.

It is good practice to document any decisions you have taken regarding the sharing of personal data without the individual's knowledge, including the reasons for those decisions. This is important in case there is a challenge to your decision to share data, for example in the form of a complaint to the ICO or a claim for compensation in the courts.

Ad hoc or 'one off' sharing

As explained above, the exemptions in the DPA can provide a basis for ad hoc sharing to take place legally in certain circumstances.

Sometimes there may be a need to share very sensitive information, even without the individual's knowledge. Acting appropriately in situations like this depends primarily on the exercise of professional judgement. However, disclosures of personal data in situations like this are still subject to the DPA. The ICO will give due weight to compliance with authoritative professional guidance in determining whether there has been a breach of the DPA. Therefore it is very much in the interests of organisations and individual employees to be aware of any professional guidance or ethical rules that are likely to be relevant to the type of decisions about disclosing personal data that they may be asked to make. It may not always be possible to document the sharing in an emergency or time dependent situation, however it is good practice to make a record as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place.

Mergers and takeovers

Where an organisation is taken over, merged, abolished or loses responsibility for carrying out a particular function, personal data might need to be shared in a way that was not originally envisaged by the organisation or individuals themselves. The DPA does not prevent organisations sharing data in these circumstances. The key point is that the use of personal data must continue to be fair.

If you know you are going to be taken over, merged with another organisation or that you are losing responsibility for carrying out a particular function, you should take steps to confirm what personal data you currently hold and establish the purposes for which the information was originally obtained.

When it becomes clear that the takeover or merger is going ahead you should consider when and how you will make individuals aware of what is happening. In some cases publicising the change will be sufficient, for example by taking out an advert in a local newspaper. In other situations it will be appropriate for an organisation to contact individuals directly to let them know what is happening. This might be necessary, for example where you have a customer relationship with individuals or where the data you hold is sensitive. In these cases there may be a particular need to reassure people that the information will still be used for the same purposes and will be kept securely.

The information you provide should identify the new organisation and remind individuals about what you hold and how it is used. This might be achieved by providing individuals with a copy of the privacy notice. The important point is that individuals understand who is holding their data and are reassured that it will continue to be used in the way they have been told about and expect.

In some cases individuals will have no real choice about whether their details are passed onto a new organisation. This might be, for example, when responsibility for providing a service they receive from the Council is passed to another organisation. In other cases individuals will have a choice about whether they continue to deal with an organisation after a merger or takeover. Where individuals do have a choice about their details being used by a new organisation, this should be made clear.

It is important that the new organisation processes individuals' data in line with their reasonable expectations. For example, if an individual has previously opted out of direct marketing this objection should be passed on and continue to be respected by the new organisation.

For example, two animal welfare charities decide to merge. They write to their members and tell them about the merger. The letter reassures members that their personal data will continue to be used for the same purposes. They also provide members with a print out of the information they currently hold about them and the marketing preferences they have on file. They ask members to let them know if any of the information needs updating.

On a practical level it can be difficult to manage records after a merger or takeover where an organisation is using different databases, or trying to integrate different systems. It is particularly important in this period that you consider the requirements of the DPA. This will include taking appropriate steps to ensure records are accurate and up to date, that you adhere to a consistent retention policy for all records and that you have appropriate security in place.

Buying and selling databases

We have produced specific guidance for organisations wanting to buy or sell customer databases: www.ico.gov.uk

Emergency response planning

In emergency response situations where there is less time to consider issues in detail it can be particularly difficult to make judgements about whether information can be shared. 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, organisations likely to be involved in responding to emergency situations should consider the types of data they are likely to need to share in advance. This should help to establish what relevant data each organisation holds and help prevent any delays in an emergency.

For 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. As part of the process they determine what type of personal data they each hold and put in place a data sharing agreement setting out what they will share and how they will share it in the event of an emergency.

For more detailed guidance in this area see 'Data Protection and Sharing – Guidance for Emergency Planners and Responders': www.cabinetoffice.gov.uk

7 Security

The Data Protection Act (DPA) requires organisations to have appropriate technical and organisational measures in place when sharing personal data. Organisations may be familiar with protecting information they hold themselves, but establishing appropriate security in respect of shared information may present new challenges.

It is good practice to take the following measures in respect of information that you share with other organisations, or that other organisations share with you.

- Review what personal data your organisation receives from other organisations, making sure you know its origin and whether any conditions are attached to its use.
- Review what personal data your organisation shares with other organisations, making sure you know who has access to it and what it will be used for.
- Assess whether you share any data that is particularly sensitive. Make sure you afford this data a suitably high level of security.
- Identify who has access to information that other organisations have shared with you; 'need to know' principles should be adopted. You should avoid giving all your staff access to shared information if only a few of them need it to carry out their job.
- Consider the effect a security breach could have on individuals.
- Consider the effect a security breach could have on your organisation in terms of cost, reputational damage or lack of trust from your customers or clients. This can be particularly acute where an individual provides their data to an organisation, but a third party recipient organisation then loses the data.

You should aim to build a culture within your organisation where employees know and understand good practice, in respect of 'its own' data and that received from another organisation. Staff should be aware of security policies and procedures and be trained in their application. In particular you will need to:

- design and organise your security to fit the type of personal data you disclose or receive and the harm that may result from a security breach;
- be clear about which staff members in the organisations involved in the sharing are responsible for ensuring information security. They should meet regularly to ensure appropriate security is maintained;

- have appropriate monitoring and auditing procedures in place; and
- be ready to respond to any failure to adhere to a data sharing agreement swiftly and effectively.

Physical security

Do you have good quality access control systems for your premises?

How are visitors supervised?

Is paper based information stored and transferred securely?

Are laptops and removable media such as discs and memory sticks locked away at night?

Do you dispose of paper waste securely, for example by shredding?

Do you advise staff on how to use their mobile phones securely and minimise the risk of them being stolen?

Technical security

Is your technical security appropriate to the type of system you have, the type of information you hold and what you do with it?

If you have staff that work from home, do you have security measures in place to ensure that this does not compromise security?

How is encryption of personal data implemented and managed?

Have you identified the most common security risks associated with using a web-product – e.g. a website, web application or mobile application?

How do you control access to your systems?

Do you set privileges to information based on people's need to know?

What measures are in place for the security of information in transit?

When personal data is shared, it is good practice for the organisation disclosing it to make sure that it will continue to be protected with adequate security by any other organisations that will have access to it. The organisation disclosing the information should ensure that the receiving organisation understands the nature and sensitivity of the information. It is good practice to take reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement. Please note, though, that the organisations the data is disclosed to will take on their own legal responsibilities in respect of the data, including its security.

Difficulties can arise when the organisations involved have different standards of security and security cultures or use different protective marking systems. It can also be difficult to establish common security standards where there are differences in organisations' IT systems and procedures. Any such problems should be resolved before any personal data is shared.

There should be clear instructions about the security steps which need to be followed when sharing information by a variety of methods, for example phone, fax, email or face to face.

8 Governance

Responsibility

The various organisations involved in a data sharing initiative will each have their own responsibilities, and liabilities, in respect of the data they disclose or have received. The issues the data sharing is intended to address may be very sensitive ones, and the decisions staff members may have to take can call for great experience and sound judgement. Therefore it is good practice for a senior, experienced person in each of the organisations involved in the sharing to take on overall responsibility for information governance, ensuring compliance with the law, and providing advice to staff faced with making decisions about data sharing.

Data sharing agreements

Data sharing agreements – sometimes known as 'data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

A data sharing agreement should, at least, document the following issues:

- the purpose, or purposes, of the sharing;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- the data to be shared;
- data quality – accuracy, relevance, usability etc;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- sanctions for failure to comply with the agreement or breaches by individual staff.

Section 14 of this document sets out the key elements of a data sharing agreement.

Privacy impact assessments (PIAs)

Before entering into any data sharing arrangement, it is good practice to carry out a privacy impact assessment. This will help you to assess the benefits that the data sharing might bring to particular individuals or society more widely. It will also help you to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. As well as harm to individuals, you may wish to consider potential harm to your organisation's reputation which may arise if data is shared inappropriately, or not shared when it should be. Privacy impact assessments are mandatory for UK Central Government Departments when introducing certain new processes involving personal data. Further information on privacy impact assessments can be found on our website at: www.ico.gov.uk

Please see the Ministry of Justice's guidance for Central Government Departments on PIAs at: www.justice.gov.uk

Data standards

The Data Protection Act (DPA) principles (see Annex 1) provide a framework which organisations involved in data sharing should use to develop their own information governance policies. It is important to have procedures in place to maintain the quality of the personal data you hold, especially when you intend to share data. When you are planning to share data with another organisation, you need to consider all the data quality implications.

When sharing information, you should consider the following issues:

- **Make sure that the format of the data you share is compatible with the systems used by both organisations.**

Different organisations may use very different IT systems, with different hardware and software and different procedures for its use. This means that it can be very difficult to 'join' systems together in order to share personal data properly. These technical issues need to be given due weight when deciding whether, or how, to share personal data.

Organisations may also record the same information in different ways. For example, a person's date of birth can be recorded in various formats. This can lead to records being mismatched or becoming corrupted. There is a risk that this will cause detriment to individuals if holding an incomplete record means that you do not provide services correctly. Before sharing information you must make sure that the organisations involved have a common way of recording key information, for example by deciding on a standard format for recording people's names. A relatively common problem here is the recording of names which contain non-Latin characters. Each organisation might have its own way of recording these, depending on the capabilities of its system. If you cannot establish a common standard for recording information, you must develop a reliable means of converting the information.

If the characters in a dataset are encoded using a different system, they might not transfer correctly. You should ensure that the data is compatible with both systems, especially in cases which are more likely to use non-standard characters.

Given the problems of interoperability that can arise, it is good practice for organisations that are likely to be involved in data sharing to require common data standards as part of their procurement exercises. IT suppliers should be made aware of these requirements.

The government data standards catalogue is here: www.cabinetoffice.gov.uk

For local government: http://standards.esd.org.uk

For the NHS: www.connectingforhealth.nhs.uk

- **Check that the information you are sharing is accurate before you share it.**

Before you share data you should take steps to check its accuracy. After the information has been shared it can be difficult to have it amended, so you should do as much as you can prior to disclosure. The steps you take should depend on the nature of the data involved. If you are sharing sensitive data and any inaccuracy would potentially harm the data subject, you will need to take extra care to ensure that the information is correct.

It is good practice to check from time to time whether the information being shared is of good quality. For example, a sample of records could be looked at to make sure the information contained in them is being kept up to date. The larger the scale of the data sharing, the more rigorous the sampling exercise should be. It is a good idea to show the records to the people they are about so that the quality of information on them can be checked. Although this may only reveal deficiencies in a particular record, it could indicate wider systemic failure that can then be addressed.

- **Establish ways for making sure inaccurate data is corrected by all the organisations holding it.**

You should ensure that procedures are in place for amending data after it has been shared. This might be because the data subject notifies you of an inaccuracy, or because they have asked you to update their details. The action you need to take will depend on the circumstances of each case. If the data is intended for ongoing use then it could be necessary for all the organisations holding it to amend it.

If several organisations are sharing information in a partnership, they should establish who is responsible for maintaining the accuracy of the data and responding to any complaints or requests for amendment.

- **Agree common retention periods and deletion arrangements for the data you send and receive.**

The various organisations sharing personal data should have an agreement about what should happen once the need to use the data has passed. Where the information is held electronically the information should be deleted, and a formal note of the deletion should be sent. Where the particular issue that the data sharing was intended to deal with has been resolved, all the organisations involved should delete their copies of the information unless there is a requirement to retain it for another purpose, for example archiving. Paper records can cause particular problems. It can be easy to overlook the presence of old paper records in archives or filing systems – and they may well contain personal data subject to the DPA. Once the need to retain them has passed, paper records should be securely destroyed or returned to the organisation they came from.

The various organisations involved in a data sharing initiative may need to set their own retention periods for information, perhaps because they work to different statutory retention periods. However, if shared data is no longer needed for the purpose for which it was shared, then all the organisations it was shared with should delete it. However, the organisation, or organisations, that collected the data in the first place may be able, or be required, to retain the original data for another legitimate purpose.

Some information will be subject to a statutory retention period and this must be adhered to. You must make sure that any organisation that has a copy of the information also deletes it in accordance with statute.

If you can remove all identifying information from a dataset so that it no longer constitutes personal data, then it can be retained indefinitely.

- **Train your staff so that they know who has the authority to share personal data, and in what circumstances this can take place.**

It is essential to provide training on data sharing to staff that are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role in respect of the sharing of personal data. It can be incorporated into any training you already give on data protection, security, or legal obligations of staff.

Different types of staff involved in data sharing will have different training needs, depending on their role. Those who:

- plan and make decisions about systematic sharing;
- administer systems; or
- make decisions in one off situations

will each have different requirements based on their responsibilities.

The focus of the training should be enabling staff to make informed decisions about whether or how to share data, and how to treat the data they are responsible for.

People who have overall responsibility for data sharing need to understand:

- the relevant law surrounding data sharing, including the DPA;
- any relevant professional guidance or ethical rules;
- data sharing agreements and the need to review them;
- how different information systems work together;
- security and authorising access to systems holding shared data;
- how to conduct data quality checks; and
- retention periods for shared data.

They also need the seniority and influence to make authoritative decisions about data sharing.

Reviewing your data sharing arrangements

Once you have a data sharing arrangement in place you should review it on a regular basis. This is because changes can occur and they need to be reflected in your arrangements to ensure that such sharing can still be justified. If it cannot be justified, it should stop.

You should ask yourself the following key questions regularly:

- Is the data still needed? You may find that the aim of the data sharing has been achieved and that no further sharing is necessary. On the other hand, you may find that the data sharing is making no impact upon your aim and therefore the sharing is no longer justified.
- Do your privacy notice and any data sharing agreements you have in place still explain the data sharing you are carrying out accurately? Please see the fairness and transparency section of this code and section 14 on data sharing agreements for further information.

- 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 whether anonymised information could be used instead;
  - that only the minimum amount of data is being shared and that the minimum number of organisations, and their staff members, have access to it;
  - that the data shared is still of appropriate quality;
  - that retention periods are still being applied correctly by all the organisations involved in the sharing;
  - that all the organisations involved in the sharing have attained and are maintaining an appropriate level of security; and
  - that staff are properly trained and are aware of their responsibilities in respect of any shared data they have access to.
- Have you checked that you are still providing people with access to all the information they're entitled to, and that you're making it easy for them to access their shared personal data?
- Have you checked that you are responding to people's queries and complaints properly and are analysing them to make improvements to your data sharing arrangements?

If significant changes are going to be made to your data sharing arrangements, then those changes need to be publicised appropriately. This can be done by updating websites, sending emails directly to people or, if appropriate, placing advertisements in local newspapers.

9 Individuals' rights

The Data Protection Act (DPA) gives individuals certain rights over their personal data. These include:

- the right to access personal data held about them;
- the right to know how their data is being used; and
- the right to object to the way their data is being used.

Access to information

Organisations are required by law to give people access to data about them in a permanent form. For most records, you can charge a fee of £10. You can find more advice on responding to requests in our Guide to data protection: www.ico.gov.uk

- You should provide clear information for individuals about how they can access their data and make this process as straightforward as possible.
- You must be able to locate and access personal data you are responsible for promptly in order to respond to requests.
- When you receive a request from an individual for their personal data you must respond to the request promptly and in any event within 40 days.

When several organisations are sharing personal data it may be difficult for an individual to decide who they should make a request for information to. You should provide clear information about the way in which individuals can make requests. It is good practice to provide a single point for individuals to direct their access requests to, allowing them to access the data that has been shared between several organisations without making multiple requests. This should also allow individuals to pay a flat fee of £10, rather than paying a number of organisations £10 each.

It is good practice to provide ways for people to access and check their own data without needing to make a formal request. You could do this by setting up facilities to allow records to be viewed online, if this can be done securely, or by showing people their data when you are in contact with them. Providing these options could save you time responding to formal requests and help to ensure the data you hold is accurate and up to date.

Where personal data is shared between several bodies it can be difficult to determine who is responsible for the data and what exactly is held. It is very important that organisations sharing data

manage their records well to ensure they can locate and provide all the data held about a person when they receive an access request.

When responding to a request for personal data an organisation is also required by law to provide a description of the purposes for which the data is held and details of the recipients or types of recipients that the data is disclosed to. Providing this information is particularly important where data is being shared, so that individuals are reminded about the ways their information is being used and disclosed. It also makes it easier for them to take action where they think an organisation has disclosed their data to another organisation inappropriately.

You are also required to provide any information you have about the source of the data you hold. In some cases this information may have been provided by another individual. This might be the case, for example, where a child's social work file contains information provided by a concerned neighbour. In cases like this, there is likely to be a clear basis for information about the source to be withheld. Our guidance on 'Subject access and other people's information' contains more detail on this subject: www.ico.gov.uk

In certain cases you may be responsible for replying to a request for personal data which was shared with you but you may not be in a position to make the judgement about whether a particular exemption to withhold data should be applied. For example, you may be concerned about the impact of releasing a report containing information prepared by a doctor about an individual's health. The decision about whether disclosing this information could cause serious harm to the individual would need to be made by a medical professional. In this instance you would need to seek advice from the doctor who prepared the report or another medical professional if this is not possible.

Individuals' objections

Individuals can object where the use of their personal data is causing them substantial, unwarranted damage or substantial, unwarranted distress. The objection can be to a particular use of information or to the fact an organisation is holding their personal data at all. Organisations are required by law to respond to individuals who object in writing to the way their personal data is being used. However they do not need to comply with the request unless there is damage or distress and this is substantial and unwarranted.

You could avoid objections by providing individuals with clear information about the basis on which you are sharing their personal data and the ways it will be used.

- When you receive a request from an individual to stop using their information you must respond to them within 21 days to confirm what action you intend to take.
- If you consider their objection unwarranted you should let them know and provide clear reasoning for your decision.

- If you are taking action to comply with the individual's request you should explain the steps you are going to take and provide a timescale.

In the DPA the right to object is linked to the likelihood of substantial and unwarranted damage or distress being caused. This means that this section of the DPA does not provide the individual with an unqualified right to stop their personal data being shared.

Queries and complaints

Individuals may have queries or complaints about how their personal data is being shared, particularly where they think the data is wrong or that the sharing is having an adverse effect on them. It is good practice to have procedures in place to deal with any queries or comments you receive in a quick and helpful way, for example by having a single point of contact for members of the public. It is good practice to analyse the comments you receive in order to develop a clearer understanding of public attitudes to the data sharing you carry out. Answering individuals' queries can also allow you to provide further information about your data sharing, in addition to what's contained in your privacy notice.

If you inform people about your data sharing and then receive a significant number of objections, negative comments or other expressions of concern, you should review the data sharing in question. In particular, you should analyse the concerns raised and decide whether the sharing can go ahead in the face of public opposition, for example because you are under a legal obligation to share the data. Alternatively, you may need to reduce the amount of data you share or share it with fewer organisations. In large scale data sharing operations, it is good practice to set up focus groups to explore individuals' concerns and to develop more publicly acceptable ways of dealing with the issues that the data sharing was intended to address.

10 Things to avoid

When sharing personal data there are some practices that you should avoid. These practices could lead to regulatory action:

- Misleading individuals about whether you intend to share their information. For example, not telling individuals you intend to share their personal data because you think they may object.
- Sharing excessive or irrelevant information about people. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is being shared for.
- Sharing personal data when there is no need to do so – for example where anonymised statistical information can be used to plan service provision.
- Not taking reasonable steps to ensure that information is accurate and up to date before you share it. For example, failing to update address details before sharing information, leading to individuals being pursued at the wrong address or missing out on important information.
- Using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data.
- Having inappropriate security measures in place, leading to loss or unauthorised disclosure of personal details. For example, sending personal data between organisations on an unencrypted memory stick which is then lost or faxing sensitive personal data to a general office number.

11 ICO powers and penalties

The ICO aims to make compliance with the Data Protection Act (DPA) easier for the majority of organisations who want to handle personal data well. In cases where organisations do not comply the ICO has powers to take action to change behaviour. These powers include the ability to serve an enforcement notice, to conduct audits and to serve a monetary penalty notice. The tools are not mutually exclusive. They will be used in combination where justified by the circumstances.

The main options are:

- **Information notice:** this requires organisations to provide the ICO with specified information within a certain time period.
- **Undertaking:** this commits an organisation to a particular course of action in order to improve its compliance with the DPA.
- **Enforcement notice:** this compels an organisation to take the action specified in the notice to bring about compliance with the DPA. For example, a notice may be served to compel an organisation to start complying with subject access requests in the timescale required or a notice may require an organisation to take steps to prevent security breaches. Failure to comply with an enforcement notice can be a criminal offence.
- **Monetary penalty notice:** a monetary penalty notice requires an organisation to pay a monetary penalty of an amount determined by the ICO, up to a maximum of £500,000. This power can be used if:
  - an organisation has seriously contravened the data protection principles; and
  - the contravention was of a kind likely to cause substantial damage or substantial distress.

In addition the contravention must either have been deliberate or the organisation must have known, or ought to have known, that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

More guidance on the circumstances in which the Information Commissioner will use this power, including what is considered a 'serious breach', can be found in our guidance: www.ico.gov.uk

- **Audit:** the ICO can conduct consensual or compulsory audits (following the serving of an Assessment Notice). A compulsory audit would be used by the ICO to determine whether an organisation has complied or is complying with the data protection principles where risks are identified and an organisation is unwilling to consent to an audit.

A consensual audit can assess an organisation's processing of personal data for the following of good practice. This includes a consideration of the legal requirements of the DPA and other relevant ICO codes and guidance. This will include the requirements of this code of practice.

The power to undertake compulsory audits currently only extends to government departments. However, other sectors may be designated by order of the Secretary of State.

The 'Assessment notices code of practice' sets out the factors which will be considered when the ICO decides whether to pursue a compulsory audit and specifies how that audit process will be conducted: www.ico.gov.uk

The ICO takes a selective, proportionate and risk based approach to pursuing regulatory action. Action is driven by concerns about actual or potential detriment caused by failure to comply with the DPA. The factors the ICO will take into account in determining whether regulatory action is appropriate are listed in the Data Protection Regulatory Action Policy: www.ico.gov.uk

12 Notification

The Data Protection Act (DPA) requires that organisations provide the ICO with a description of the individuals or organisations to whom they intend or may wish to disclose personal data. The legal requirement is to provide a description of the recipient or the recipients of the data – this means types of organisation, not the names of specific organisations. The notification requirement does not include people to whom you may be required by law to disclose personal data in a particular case, for example where the police require a disclosure of personal data under a warrant.

When you intend to share personal data with another organisation or group of organisations you must check whether you need to update your notification to describe this. When any part of the notification entry becomes inaccurate or incomplete, for example because you are now disclosing information to a new type of organisation, you must inform the ICO as soon as practical and in any event within 28 days. It is a criminal offence not to do this.

Where several organisations are sharing personal data it is important that each organisation is clear about the personal data they are responsible for and include that information on their notification entry.

You can find out whether you need to notify under the DPA here: www.ico.gov.uk

13 Freedom of Information

The Freedom of Information Act 2000 (FOIA) gives everyone the right to ask for information held by a public authority and, unless exempt, to be told whether the information is held and to be provided with the information. In some cases, public authorities can refuse to confirm or deny whether they hold requested information. Advice on which organisations are public authorities under the Act can be found on our website at: www.ico.gov.uk

The INSPIRE Regulations contain provisions that deal specifically with the sharing of spatial data sets and spatial data services between public authorities. For more information about this see: www.legislation.gov.uk

The FOIA requires every public authority to adopt and maintain a publication scheme, which is a commitment to publish information on a proactive and routine basis. This supports the culture of transparency introduced by freedom of information legislation and allows the public to easily identify and access a wide range of information without having to make a request.

This section relates to the FOIA and does not apply to Scottish public authorities, which are subject to the Freedom of Information (Scotland) Act 2002 (FOISA). Further information on the freedom of information obligations of Scottish public authorities, including requirements with regard to publication schemes, can be found on the website of the Scottish Information Commissioner at: www.itspublicknowledge.info

Most, if not all, public sector bodies involved in data sharing are subject to freedom of information law. This means they are required to publish information in accordance with their publication scheme. The ICO introduced a model publication scheme that should be adopted by all public authorities subject to FOIA. The scheme became available for adoption on 1 January 2009. Further information on the scheme can be found on our website at: www.ico.gov.uk

Public authorities are required to publish information covered by the model scheme's seven classes, and in accordance with class 5 they are required to publish their policies and procedures. In most cases this will include the policies and procedures relating to data sharing, including the details of the organisations with which data is shared and any relevant code of practice. Further information on the types of information we expect public authorities to make available through their schemes is available on our website at: www.ico.gov.uk

There is a strong public interest in members of the public being able to find out easily why data is being shared, which organisations are involved and what standards and safeguards are in place. Making your policies and procedures available to the public proactively should help to reassure individuals and to establish an increased level of trust and confidence in your organisation's data sharing practices. You should consider including details of data sharing with other public authorities within the policies and procedures that you publish in accordance with your publication scheme.

There will often be cases where data is shared with other public authorities. This will usually mean that the data is held for the purposes of the FOIA by all the data sharing partners and an FOI request could be made to any of the public authorities that hold the information. However, within the FOIA there is an exemption for the personal data of third parties that falls within the scope of a request. In many cases this exemption will apply as disclosure is likely to be unfair and so be in breach of the first data protection principle.

Often people will make requests for information that cover both personal and non-personal data. For example, a person may request data about them that is being shared between various agencies and information about those agencies' policies for sharing information. Data protection and freedom of information may be dealt with by separate parts of your organisation, and a hybrid request may have to be dealt with under both pieces of legislation. However, it is good practice to be as helpful as possible when dealing with requests of this sort, especially as members of the public may not understand the difference between a data protection and an FOI request.

There may be circumstances where a private or third sector organisation shares data with a public authority. It is therefore important that, in such cases, individuals are made aware that information they provide will also be held by an organisation that is subject to the FOIA and so may fall within the scope of a request for information made to the public authority. However, as mentioned previously, there is an exemption within the FOIA for the personal data of third parties to which a request for information relates. In many cases this exemption will apply as disclosure is likely to be unfair and so be in breach of the principle that personal data must be processed fairly and lawfully.

14 Data sharing agreements

Data sharing agreements can take a variety of forms, depending on the scale and complexity of the data sharing in question. You should remember that a data sharing agreement is a set of common rules binding on all the organisations involved in a data sharing initiative. This means that the agreement should be drafted in clear, concise language that is easily understood.

Drafting and adhering to an agreement does not in itself provide any form of legal indemnity from action under the Data Protection Act (DPA) or other law. However, an agreement should help you to justify your data sharing and to demonstrate that you have been mindful of, and have documented, the relevant compliance issues. The ICO will take this into account should it receive a complaint about your data sharing.

In order to adopt good practice and to comply with the DPA, the ICO would expect a data sharing agreement to address the following issues:

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. This should be documented in precise terms so that all parties are absolutely clear as to the purposes for which data may be shared and shared data may be used.

The organisations that 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 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.

Data items to be shared:

Your agreement should explain the types of data that 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 certain details held in a file about someone, but not other, more sensitive, material. In some cases it may be appropriate to attach 'permissions' to certain data items, so that only certain members of staff, for example ones that have received appropriate training, are allowed to access them.

Basis for sharing:

You need to explain your basis for sharing data clearly. If you are a public sector body, you may be under a legal duty to share certain types of personal data. Even if you are not under any legal requirement to share data, you should explain the legal power you have which allows you to share. If you are a private or third sector organisation then you may not need a specific legal power to disclose personal data, but your agreement should still explain how the disclosures will be consistent with the DPA.

If consent is to be a basis for disclosure then your agreement could provide a model consent form. It should also address issues surrounding the withholding or retraction of consent.

Access and individuals' rights:

The agreement should explain what to do when an organisation receives a DPA or FOIA request for access to shared data. In particular, it should ensure that one staff member or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared data easily. Although decisions about access will often have to be taken on a case by case basis, your agreement should give a broad outline of the sorts of data you will normally release in response to either DPA or FOIA requests. It should also address the inclusion of certain types of information in your FOIA publication scheme.

Information governance:

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 may be shared, to prevent irrelevant or excessive information being disclosed;
- make sure that the data being shared 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 – for example dates of birth – should be recorded;
- 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 for the transmission of the data and procedures for dealing with any breach of the agreement;

- have procedures for dealing with DPA or FOIA access requests, or complaints or queries, from members of the public;
- have a timescale for assessing the ongoing effectiveness of the data sharing initiative and of 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.

It might be helpful for your agreement to have an appendix, including:

- a glossary of key terms;
- a summary of the key legislative provisions, for example relevant sections of the DPA, any legislation which provides your legal basis 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
- a data sharing decision form.

Template 'data sharing request' form

Name of organisation:	
Name and position of person requesting data:	
Date of request:	
Reference to data sharing agreement:	
Data requested:	
Purpose:	
Date required by:	
Any specific arrangements re: retention/deletion of data:	
Signed:	
Dated:	

Template 'data sharing decision' form

Name of organisation:	
Name and position of person requesting data:	
Date request received:	
Data requested:	
Purpose:	
Decision:	
Data supplied:	
Reason(s) for disclosure or non-disclosure:	
Any specific arrangements re: retention/deletion of data:	
Decision taken by (name and position):	
Date of disclosure:	
Signed:	
Dated:	

15 Data sharing checklists

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?
Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example, was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Data sharing checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?
Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision
Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Annex 1 – The data protection principles

1. "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".
2. "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".
3. "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".
4. "Personal data shall be accurate and, where necessary, kept up to date".
5. "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".
6. "Personal data shall be processed in accordance with the rights of data subjects under this Act".
7. "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".
8. "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

Annex 2 – Glossary

Anonymised information – information from which no individual can be identified.

Assessment notice – this gives the Information Commissioner certain powers to assess compliance with the Data Protection Act.

Data controller – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor – any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Act 1998 (DPA) – the main UK legislation which governs the handling and protection of information relating to living people.

Data sharing – the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

Data sharing agreements/protocols – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

Interoperability – in relation to electronic systems or software, the ability to exchange and make use of information.

INSPIRE Regulations – Directive 2007/2/EC of the European Parliament and of the Council establishing an Infrastructure for Spatial Information in the European Community.

Notification – The Information Commissioner's Office maintains a public register of data controllers. Each register entry includes the name and address of the data controller and details about the types of personal data they process. Notification is the process by which a data controller's details are added to the register.

Personal data – data which relate to a living individual who can be identified—

a from those data, or

b from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy impact assessment (PIA) – is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Processing of data – in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

a organisation, adaptation or alteration of the information or data,

b retrieval, consultation or use of the information or data,

c disclosure of the information or data by transmission, dissemination or otherwise making available, or

d alignment, combination, blocking, erasure or destruction of the information or data.

Public authority – as defined in section 3 of the Freedom of Information Act 2000.

Sensitive personal data – personal data consisting of information as to—

a the racial or ethnic origin of the data subject,

b his political opinions,

c his religious beliefs or other beliefs of a similar nature,

d whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

e his physical or mental health or condition,

f his sexual life,

g the commission or alleged commission by him of any offence, or

h any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Subject access request (SAR) – under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records, by writing to the person or organisation they believe holds it. A subject access request must be made in writing (email is acceptable) and must be accompanied by the appropriate fee, usually up to a maximum of £10. Once the applicable fee has been paid, a reply must be received within 40 calendar days.

Third sector – non-governmental, not for profit organisations such as charities, voluntary and community organisations and social enterprises.

Annex 3 – Case studies

A group of retailers has set up a national database containing the details of former employees who were dismissed for stealing from their employer. This will allow employers participating in the scheme to vet job applicants as part of the recruitment process.

- Each participating retailer's privacy notice should explain, in general terms, that information about employees dismissed for theft will be included on the database.
- Given the significant effect the information on the database could have on their employment prospects, individuals should be told that their details have been included on it, using the most up to date details the retailer has.
- Individuals should be allowed to check that the information held about them is correct and either have it corrected or deleted, or have a note saying that they disagree with the information included on their record.

It would be the individual's prerogative to seek compensation if an employment prospect is denied them on the basis of inaccurate personal data.

A group of police forces are cooperating with immigration officials to collect evidence about a number of individuals thought to be involved in people trafficking. This involves exchanging data about suspects' whereabouts and activities.

- There is no need to tell any of the suspects that personal data about them is being collected or exchanged. This is because doing so would 'tip off' the suspects, allowing them to destroy evidence, prejudicing the likelihood of prosecution.
- The police, or immigration agency, may still need to provide subject access to the data, and explain their collection and sharing of the data, when doing so will no longer prejudice the prosecution.

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

- Customers should have access to a privacy notice – either from the supermarket or the card scheme operator – that provides an explanation, in general terms, of the sorts of circumstances in which information about scheme members will be shared with a third party, such as the police.
- Where information about a particular scheme member has been disclosed, the supermarket does not need to inform the individual of the disclosure if this would prejudice crime prevention.

Two neighbouring health authorities want to share information about their employees because they have been informed that certain individuals are apparently being employed by both health authorities and are working the same shift pattern at each.

- The health authorities involved should make it clear to their staff that they are carrying out an anti-fraud operation of this sort. They should explain what data will be shared, who it will be shared with and why it is being shared.
- If possible, the health authorities should only share data about particular employees who are suspected of fraudulent behaviour.
- However, if data about all employees is to be matched, any discrepancies should be recorded and investigated, and data about all the other employees should be deleted or returned to the original health authority.

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

- Customers should be informed when they open the account that information will be shared with credit reference agencies.
- Credit reference agencies need to be able to link records to the correct individual. The mobile phone company should ensure it is collecting adequate information to distinguish between individuals, for example dates of birth.
- The organisations involved should have procedures in place to deal with complaints about the accuracy of the information they have shared.

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 free school meals. Therefore, it wants to ask all local primary and secondary schools for 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 benefit, can be inferred fairly reliably from a child's receipt of free school meals. 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.
- 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 and seeking their consent for the sharing of the data.
- Alternatively, the school could disclose an anonymised data set, or statistical information, to the researchers.
- There is an exemption from subject access for data processed only for research purposes, provided certain conditions are satisfied, for example the research results are not made available in a form which identifies anyone. However, it is good practice to provide data subjects with access to their personal data wherever possible. If subject access is going to be refused, for example because giving access would prejudice the research results, this should be explained to individuals during the research enrolment process.

A marketing company (data controller) wants to share data with a 'fulfilment' company (data processor) so it can send out free samples and information about special offers to its customers. Before it supplies its customers' data to the fulfilment company the marketing company must:

- make sure the fulfilment house can guarantee sufficient technical and organisational security;
- put a contract in place saying what the fulfilment company can and cannot do with the personal data supplied to it, and imposing security requirements on it; and
- take reasonable steps to ensure sufficient security is being maintained.

A local authority's Recreation Department wants to promote take up of a new keep fit service for disabled people that it has launched at a local sports centre. The Authority's Revenue Department holds records of people who are eligible for reduced Council Tax on account of a disability. The Recreation Department wants a list of these people, so it can send them a leaflet promoting the new keep fit service.

- Many people will consider information about their health, particularly their disability, to be particularly sensitive. Therefore they might find it inappropriate for the Revenue Department to have shared their details with the Recreation Department.
- The sharing of data could be avoided if the Revenue Department sends out the promotional leaflet on behalf of the Recreation Department. However, some Council Tax payers might still find this inappropriate.
- Council Tax information is collected under statutory authority so the Revenue Department should seek legal advice before using the information for a non-Council Tax related purpose.

A council is outsourcing work previously carried out by its children and family services department to a charity. The charity will need details of the families currently receiving services to take over the council's role. The council writes to customers to tell them what is happening. As customers have no option but to deal with the new provider if they want to continue to receive their services, the council's letter should explain clearly who will be providing the service and what information will be passed over. It should reassure customers that information will continue to be used for the same purposes.

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 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.

If you would like to contact us please call 0303 123 1113

www.ico.org.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

May 2011

ico.
Information Commissioner's Office

Upholding information rights