The Guide to Data Protection



ico.
Information Commissioner's Office

About the guide 3
Key definitions 4
Data protection principles 15
Principle 1 – fair and lawful 16
Principle 2 – purposes 23
Principle 3 – adequacy 26
Principle 4 – accuracy 30
Principle 5 – retention 37
Principle 6 – rights 43
Subject access request 44
Damage or distress 57
Preventing direct marketing 62
Automated decision taking 67
Correcting inaccurate personal data 70
Compensation 73
Principle 7 – security 75
Principle 8 – international 83
Conditions for processing 98
Exemptions 103
Complaints 114
Anonymisation 115
Big data 117
CCTV 119
Data sharing 121
Employment 123
Online and apps 125
Privacy by design 129

About the guide

About the Guide to data protection

This guide is for those who have day-to-day responsibility for data protection.

It explains the purpose and effect of each principle, gives practical examples and answers frequently asked questions.

It also contains specialist topics including CCTV, employment and data sharing.

Key definitions

In this guide we have tried as far as possible to avoid using technical terms. However, in some circumstances you will need to consider the meaning of a relevant defined term to judge whether and how the Data Protection Act applies. This section sets out the key definitions in the Act, explains what they mean, and shows how they often relate to each other.

On this page...

- What type of information is protected by the Data Protection Act?
- What is personal data?
- What activities are regulated by the Data Protection Act?
- Who has rights and obligations under the Data Protection Act?
- Who determines the "purpose and manner" of processing?
- What about processing that is required by law?
- How long do data protection rights and duties last?
- What are the other key definitions in the Data Protection Act?

What type of information is protected by the Data Protection Act?

The Act regulates the use of "personal data". To understand what personal data means, we need to first look at how the Act defines the word "data".

> **Data** means information which –
>
> (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
>
> (b) is recorded with the intention that it should be processed by means of such equipment,
>
> (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
>
> (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
>
> (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Paragraphs (a) and (b) make it clear that information that is held on computer, or is intended to be held on computer, is data. So data is also information recorded on paper if you intend to put it on computer.

Relevant filing system (referred to in paragraph (c) of the definition) is defined in the Act as:

> any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

This is not an easy definition. Our view is that it is intended to cover non-automated records that are structured in a way which allows ready access to information about individuals. As a broad rule, we consider that a relevant filing system exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals. For further guidance see the FAQs about relevant filing systems.

"Accessible record" (referred to in paragraph (d) of the definition) means:

- a health record that consists of information about the physical or mental health or condition of an individual, made by or on behalf of a health professional (another term defined in the Act) in connection with the care of that individual;
- an educational record that consists of information about a pupil, which is held by a local education authority or special school (see Schedule 11 of the Act for full details); or
- an accessible public record that consists of information held by a local authority for housing or social services purposes (see Schedule 12 for full details).

Accessible records were included in the definition of "data" because pre-existing access rights to information were not restricted to automatically processed records, or records held in non-automated systems falling within the definition of "relevant filing systems". So, to preserve all these pre-existing access rights, the definition of "data" covers accessible records even if they do not fall in categories (a), (b), or (c).

The Freedom of Information Act 2000 created a new category of data which extended the definition of "data" in the Data Protection Act to include any information held by a public authority which would not otherwise be caught by the definition. Where information requested under the FOI Act includes information about identifiable individuals, public authorities must consider whether its release would breach the Data Protection Act. The new category of data (which is often referred to as "category (e) data") is designed to ensure that before releasing any personal information under the FOI Act, public authorities consider whether this would be fair. Processing category (e) data is exempt from most of the rights and duties created by the Data Protection Act.

You can find more detailed information in:

Determining what information is data for the purposes of the DPA
For organisations
PDF (284.34K)

What is personal data?

Personal data means 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.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

Example
An organisation holds data on microfiche. The microfiche records do not identify individuals by name, but bear unique reference numbers which can be matched to a card index system to identify the individuals concerned. The information held on the microfiche records is personal data.

The definition also specifically includes opinions about the individual, or what is intended for them.

Example
A manager's assessment or opinion of an employee's performance during their initial probationary period will, if held as data, be personal data about that individual. Similarly, if a manager notes that an employee must do remedial training, that note will, if held as data, be personal data.

We have produced What is personal data? - A quick reference guide (pdf) and there is also detailed guidance Determining what is personal data (pdf).

Sensitive personal data means 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.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. In particular, if you are processing sensitive personal data you must satisfy one or more of the conditions for processing which apply specifically to such data, as well as one of the general conditions which apply in every case. The nature of the data is also a factor in deciding what security is appropriate. Please see Schedules 2 and 3 of the Act and the section of this guide on the conditions for processing.

The categories of sensitive personal data are broadly drawn so that, for example, information that someone has a broken leg is classed as sensitive personal data, even though such information is relatively matter of fact and obvious to anyone seeing the individual concerned with their leg in plaster and using crutches. Clearly, details about an individual's mental health, for example, are generally much more "sensitive" than whether they have a broken leg.

Many individuals choose to make their political allegiance public, for example by wearing badges or rosettes or by putting a sticker in their window. There is a condition for processing sensitive personal data that covers information made public by the individual concerned.

Religion or ethnicity, or both, can often be inferred with varying degrees of certainty from dress or name. For example, many surnames are associated with a particular ethnicity or religion, or both, and may indicate the ethnicity and religion of the individuals concerned. However, it would be absurd to treat all such names as "sensitive personal data", which would mean that to hold such names on customer databases you had to satisfy a condition for processing sensitive personal data. Nevertheless, if you processed such names specifically because they indicated ethnicity or religion, for example to send marketing materials for products and services targeted at individuals of that ethnicity or religion, then you would be processing sensitive personal data. In any event, you must take care when making assumptions about individuals as you could be collecting inaccurate personal data.

What activities are regulated by the Data Protection Act?

The Act regulates the "processing" of personal data.

Processing, 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.

The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing.

Who has rights and obligations under the Data Protection Act?

This guide describes how the Act protects the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers). We generally use the terms "organisation" and "you" rather than "data controller", and "individual" instead of "data subject".

However, it is important to understand:

- what these terms mean and their significance; and
- the difference between a data controller and a data processor, as they are treated differently under the Act.



Data subject means an individual who is the subject of personal data.

In other words, the data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.



Data controller means … 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.

A data controller must be a "person" recognised in law, that is to say:

- individuals;

- organisations; and
- other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

Example
A network of town-centre CCTV cameras is operated by a local council jointly with the police. Both are involved in deciding how the CCTV system is run and what the images it captures are used for. The council and the police are joint data controllers in relation to personal data processed in operating the system.

Example
A government department sets up a database of information about every child in the country. It does this in partnership with local councils. Each council provides personal data about children in its area, and is responsible for the accuracy of the data it provides. It may also access personal data provided by other councils (and must comply with the data protection principles when using that data). The government department and the councils are data controllers in common in relation to the personal data on the database.

Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.



Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Example
A utilities company engages a company which operates call centres to provide many of its customer

services functions on its behalf. The call centre staff have access to the utilities company's customer records for the purpose of providing those services but may only use the information they contain for specific purposes and in accordance with strict contractual arrangements. The utilities company remains the data controller. The company that operates the call centre is a data processor.

Data processors are not directly subject to the Act. However, most data processors, if not all, will be data controllers in their own right for the processing they do for their own administrative purposes, such as employee administration or sales.

Please see our guidance Data controllers and data processors: what the difference is and what the governance implications are (pdf). This explains how to determine whether an organisation is a data controller or a data processor, and the governance implications of a controller and processor working together to process personal data.

Example
An organisation engages a company which provides business services to administer its employee payroll function. The organisation also engages a marketing company to carry out a satisfaction survey of its existing customers. The business services company will need information about the organisation's employees, and the marketing company will need information about its customers. Both companies will be processing the information on behalf of the organisation, and so they are both data processors. However, they will also be processing personal data about their own employees and, in respect of that personal data, they will be data controllers.

Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor. Where roles and responsibilities are unclear, they will need to be clarified to ensure that personal data is processed in accordance with the data protection principles. For these reasons organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing. We have published guidance on Outsourcing - a guide for small and medium-sized businesses (pdf), which gives more advice about using data processors.

Who determines the "purpose and manner" of processing?

A person is only a data controller if, alone or with others, they "determine the purposes for which and the manner in which any personal data are processed". In essence, this means that the data controller is the person who decides how and why personal data is processed. However, we take the view that having some discretion about the smaller details of implementing data processing (ie the manner of processing) does not make a person a data controller.

Example
A Government department decides to help people in fuel poverty (the broad purpose). It also decides to use benefit records, which are clearly personal data, to identify who it will target

(arguably, the broad manner). It then commissions a private-sector company to do certain matching according to clear criteria, but allows the company to use some discretion in deciding how they do this (eg what software to use). In this example, the department would be the data controller and the company would be a data processor, even though it decides the details of the processing method.

So, when deciding who is a data controller, we place greatest weight on purpose – identifying whose decision to achieve a "business" purpose has led to personal data being processed.

We have produced more detailed guidance:

Data controllers and data processors: what the difference is and what the governance implications are

For organisations
PDF (274.96K)

What about processing that is required by law?

The Data Protection Act says:

> Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.

Our view is that this provision applies wherever there is a statutory duty that involves the publication or use of personal data. We do not think that it should be interpreted more narrowly – as applying only where there is an express statutory duty to process personal data – because obligations imposed by legislation other than the Data Protection Act do not usually refer to processing personal data.

So, if performing a legal duty necessarily involves processing personal data, the person required to process such data will be the data controller and will be legally responsible for ensuring that the processing complies with the Act.

Example
An Electoral Registration Officer is required by law to draw up, maintain and publish the electoral roll. The Data Protection Act makes it clear that the Electoral Registration Officer is a data controller for the electoral roll information.

This is the case even if processing personal data is an inevitable, but not the main, part of performing the legal duty. If performing a legal duty directly or indirectly involves processing personal data, the organisation under the duty will be the data controller in relation to such data processing.

Sometimes, an organisation is subject to a duty that requires processing personal data, but delegates its performance to another person. In these circumstances the person with the overall responsibility for achieving the purpose, or performing the function, bears the responsibilities of the data controller. We place greatest weight on purpose rather than manner of processing – identifying whose decision to achieve a business purpose (or to carry out a statutory function) has led to personal data being processed.

Example
A government department that is responsible for paying benefits to individuals contracts with a private company to administer the benefits. The question is whether the government department remains the data controller for processing personal data on benefits, regardless of the scope given to the company in deciding how to do this at a practical level. The government department retains overall responsibility for administering the provision of the benefits, so it remains the data controller.

How long do data protection rights and duties last?

Your duties under the Act apply throughout the period when you are processing personal data – as do the rights of individuals in respect of that personal data. So you must comply with the Act from the moment you obtain the data until the time when the data has been returned, deleted or destroyed. Your duties extend to the way you dispose of personal data when you no longer need to keep it – you must dispose of the data securely and in a way which does not prejudice the interests of the individuals concerned.

Changes in an organisation's circumstances do not reduce an individual's rights under the Act. Even if an organisation goes out of business, individuals are still entitled to expect that their personal data will be processed in accordance with the data protection principles. However, responsibility for ensuring this happens may shift, depending on the circumstances.

Example
A travel agency is run as a partnership by Mr A and Mr B. As a consequence of a downturn in business, the travel agency ceases trading abruptly. Its premises are locked up and its computers (which contain customer information) lie idle. Mr A and Mr B remain responsible for ensuring that their customers' personal data remains secure and that whatever happens to it complies with the Data Protection Act. This duty will continue even if the partnership is dissolved.

Example
A high-street retailer (which operates as a limited company) goes into administration. Control of the company's assets – including an extensive customer database – passes from the board of directors to the administrators, who decide to sell some of the assets. Because the administrators now control

the purpose and manner in which the database is used, they become data controllers in respect of the personal data it contains. The administrators must comply with the Data Protection Act in connection with any possible sale of the customer database.

What are the other key definitions in the Data Protection Act?

Most of the concepts explained above are defined in section 1 of the Data Protection Act. However, there are other important definitions. In particular, section 70 sets out supplementary definitions and section 71 lists provisions defining or explaining expressions used in the Act. The following is a list of some of the other defined terms used in the Act.

Inaccurate data. The Act states:

> For the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact.

Personal data may not be inaccurate if it faithfully represents someone's opinion about an individual, even if the opinion proves incorrect (for example, a doctor's medical opinion about an individual's condition). In these circumstances, the data would not need to be "corrected", but the data controller may have to add a note stating that the data subject disagrees with the opinion.

Recipient. The Act states:

> Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

The Act provides that a data controller's notification of processing must include "a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data". Data controllers must therefore provide a description of possible recipients, including employees, agents and data processors, rather than a specific list of actual recipients.

The Act also provides that an individual making a subject access request is entitled to be given "a description of the recipients or classes of recipients to whom [personal data] are or may be disclosed". This is so that individuals can have a better understanding of what is done with their personal data. However, the definition of "recipient" goes on to say, in effect, that people need not be identified as recipients just because information is disclosed to them as part of an inquiry they have legal power to make. This is to prevent an official investigation being compromised if an individual making a subject

access request is tipped off that an investigation is or soon will be under way – such as a police, customs or trading standards investigation.

> **Third party**, in relation to personal data, means any person other than –
>
> (a) the data subject,
>
> (b) the data controller, or
>
> (c) any data processor or other person authorised to process data for the data controller or processor.

The usual meaning of the term "third party" is someone other than the two main parties involved, for example someone other than the husband and wife in divorce proceedings. In relation to data protection, the main reason for this particular definition is to ensure that a person such as a data processor, who is effectively acting as the data controller, is not considered a third party

Although a data controller's employee to whom information is disclosed will be a "recipient", they will usually not be a "third party". This is because the employee will usually be acting in their employment capacity, and so will be acting on behalf of the data controller. If a data controller's employee receives personal data from their employer outside the normal course of their employment, the employee will be a third party in relation to their employer.

Example
A data controller may decide to disclose to one of its employees (Tom) personal data relating to another of its employees (Dick), for Tom to use as evidence in possible legal action (unconnected with Tom's employment). In this situation, Tom is not receiving the information in the course of his employment with the data controller, so will be a third party.

The term "third party" is used in the Data Protection Act relating to accuracy; to "fair processing"; and in two of the conditions for processing. Although the term "third party" is not used in the Act's provisions about subject access, further information can be found by reading the Subject access code of practice (pdf) and the section of this guide on Subject access request: In brief – what is an individual entitled to?

Data protection principles

Data protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:



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.

Principle 1 – fair and lawful

The Data Protection Act requires you to process personal data fairly and lawfully. This section explains how to comply with this requirement, and gives examples of good practice in handling personal data.

The requirement to process personal data fairly and lawfully is set out in the first data protection principle and is one of eight such principles at the heart of data protection. The main purpose of these principles is to protect the interests of the individuals whose personal data is being processed. They apply to everything you do with personal data, except where you are entitled to an exemption.

So the key to complying with the Data Protection Act is to follow the eight data protection principles.

Later sections of the guide deal with the other data protection principles in more detail.

In brief – what does the Data Protection Act say about handling personal data fairly and lawfully?

The Data Protection Act says that:

> 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.

This is the first data protection principle. In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

In more detail...

- What are the "conditions for processing"?
- What does fair processing mean?
- Is it possible to use or disclose personal data for a new purpose?
- Is it ever acceptable to disclose personal data to other organisations for them to use for their own purposes?

- What about disclosures that are in the best interests of the individual concerned?
- What about "privacy notices"?
- What is meant by "lawful"?

What are the "conditions for processing"?

The conditions set out in Schedules 2 and 3 to the Data Protection Act are known as the "conditions for processing". Organisations processing personal data need to be able to satisfy one or more of these conditions. This will not, on its own, guarantee that the processing is fair and lawful – fairness and lawfulness must still be looked at separately.

The conditions for processing are more exacting when sensitive personal data is involved, such as information about an individual's health or criminal record.

For further information, please read about the section of this guide on the conditions for processing, which contains an explanation of what they mean in practice.

What does fair processing mean?

Processing personal data must above all else be fair, as well as satisfying the relevant conditions for processing. "Processing" broadly means collecting, using, disclosing, retaining or disposing of personal data, and if any aspect of processing is unfair, there will be a breach of the first data protection principle – even if you can show that you have met one or more of the conditions for processing.

Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used. Transparency is always important, but especially so in situations where individuals have a choice about whether they wish to enter into a relationship with you. If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

The Data Protection Act says that information should be treated as being obtained fairly if it is provided by a person who is legally authorised, or required, to provide it.

Example

Personal data will be obtained fairly by the tax authorities if it is obtained from an employer who is under a legal duty to provide details of an employee's pay, whether or not the employee consents to, or is aware of, this.

However, to assess whether or not personal data is processed fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If the information has been obtained and used fairly in relation to most of the people it relates to but unfairly in relation to one

individual, there will be a breach of the first data protection principle.

Personal data may sometimes be used in a manner that causes some detriment to (negatively affects) an individual without this necessarily being unfair. What matters is whether or not such detriment is justified.

Example

Where personal data is collected to assess tax liability or to impose a fine for breaking the speed limit, the information is being used in a way that may cause detriment to the individuals concerned, but the proper use of personal data for these purposes will not be unfair.

Some organisations share personal data with other organisations. For example, charities working in the same field may wish to use or share supporters' information to allow reciprocal mailings. Some companies even trade in personal data, selling or renting the information. The individuals concerned must still be treated fairly. They should be told that their information may be shared, so they can choose whether or not to enter into a relationship with the organisation sharing it.

Why and how personal data is collected and used will be relevant in assessing fairness. Fairness requires you to:

- be open and honest about your identity;
- tell people how you intend to use any personal data you collect about them (unless this is obvious);
- usually handle their personal data only in ways they would reasonably expect; and
- above all, not use their information in ways that unjustifiably have a negative effect on them.

Is it possible to use or disclose personal data for a new purpose?

It depends on whether it would be fair to do so. You should explain why you want to use an individual's personal data at the outset, based on your intentions at the time you collect it. If over time you devise new ways of using that information, perhaps because of changes in technology, you will be able to use their personal data for the new purpose if it is fair to do so.

Example

A mail-order book and record seller has had some customers for many years and has regularly sent them catalogues of books and records. After a while the company also started selling audio tapes, CDs and DVDs. It is likely to be fair to start sending catalogues advertising DVDs to long-established customers, who are unlikely to be surprised that the company has diversified. However, customers are less likely to consider it reasonable if the company uses the interests they have shown by their purchases to promote another company's themed holidays (for example, holidays in Salzburg for opera buffs). Passing details of customers and their interests to other companies for marketing is likely to be unfair unless they have agreed to this.

Example

A bank records information about some of the individuals who are shareholders of its corporate account holders. It collects and holds this information to comply with its duties under anti-money laundering regulations. Unless the bank had obtained their prior consent, it would be unfair to use this information to send marketing material to the individuals concerned inviting them to open personal accounts with the bank.

As you develop the goods and services you offer, you should think about whether your customers are likely to reasonably expect you to use their personal data to offer them these products. If you are unsure about this, you should explain your intentions and, at the very least, give your existing customers an easy way to opt out. If you intend to make a significant change, such as proposing to disclose customer information to others, you will usually need to get your customers' consent.

Is it ever acceptable to disclose personal data to other organisations for them to use for their own purposes?

It depends. You may be approached by a third party seeking personal data about one of your employees or customers. For example, the police may want information in connection with an investigation, or an individual may want information to pursue legal action. In such cases, you may choose to disclose the information if the conditions of a relevant exemption are satisfied. For more information on exemptions, please see that section of this guide.

Unless one of these specific exemptions applies, individuals should generally be able to choose whether or not their personal data is disclosed to another organisation. If your intention to disclose information in this way was not made absolutely clear at the outset, at a time when the individual had the option not to proceed in their business relationship with you, then you will usually have to get the individual's consent before making such disclosures.

A decision to share personal data with another organisation does not take away your duty to treat individuals fairly. So before sharing personal data, you should consider carefully what the recipient will

do with it, and what the effect on individuals is likely to be. It is good practice to obtain an assurance about this, for example in the form of a written contract.

What about disclosures that are in the best interests of the individual concerned?

In some circumstances disclosure to another organisation may be justified in the individual's best interests, but where none of the statutory exemptions apply.

Example

A representative of a utility company calls at a property to cut off the electricity or gas. He finds that the property has been burgled and is not secure. The householder is out (and cannot be contacted). He therefore telephones the police. This is likely to involve disclosing the fact that the householder's electricity or gas is being cut off for non-payment. In such circumstances, it is reasonable to assume that, even if the householder may be embarrassed that others will know they have not paid their bills, they would be concerned about the burglary and about the protection of their property.

However, such circumstances will be exceptional and will only arise where you have good reasons to believe that disclosure is justified. It is not acceptable to seek to justify disclosing customer information without consent to another organisation for marketing on the grounds that it is in the interests of customers to receive useful offers.

What about "privacy notices"?

The Data Protection Act does not define fair processing. But it does say that, unless a relevant exemption applies, personal data will be processed fairly only if certain information is given to the individual or individuals concerned. It is clear that the law gives organisations some discretion in how they provide fair processing information – ranging from actively communicating it to making it readily available.

The oral or written statement that individuals are given when information about them is collected is often called a "fair processing notice", although our recent guidance uses "privacy notice" instead. However, it is probably helpful to avoid technical language altogether. Some of the most accessible notices for the public use phrasing such as "how we use your information".

In general terms, a privacy notice should state:

- your identity and, if you are not based in the UK, the identity of your nominated UK representative;
- the purpose or purposes for which you intend to process the information; and
- any extra information you need to give individuals in the circumstances to enable you to process the information fairly.

The last of these requirements is vague. However, because the Data Protection Act covers all sorts of

processing, it is hard to be prescriptive. When deciding whether you should give any other information in the interests of fairness, you have to take into account the nature of the personal data and what the individuals concerned are likely to expect. For example, if you intend to disclose information to another organisation, fairness requires that you tell the individuals concerned unless they are likely to expect such disclosures. It is also good practice to tell people how they can access the information you hold about them, as this may help them spot inaccuracies or omissions in their records.

When deciding how to draft and communicate a privacy notice, try to put yourself in the position of the people you are collecting information about. Ask yourself:

- do they already know who is collecting the information and what it will be used for?
- is there anything they would find deceptive, misleading, unexpected or objectionable?
- are the consequences of providing the information, or not providing it, clear to them?

We have issued a Privacy notices code of practice to help organisations draft clear privacy notices and to ensure they collect information about people fairly and transparently. The code explains that the duty to give a privacy notice is strongest when the information is likely to be used in an unexpected, objectionable or controversial way, or when the information is confidential or particularly sensitive. It also says there is no point telling people the obvious when it is already clear what their information will be used for.

Example

When an individual enters into a mobile phone contract, they know the mobile phone company will keep their name and address details for billing purposes. This does not need to be spelt out. However, if the company wants to use the information for another purpose, perhaps to enable a sister company to make holiday offers, then this would not be obvious to the individual customer and should be explained to them.





Privacy notices code of practice

This code of practice is designed to help you to collect and use information appropriately by drafting clear and genuinely informative privacy notices.

Collecting information about your customers - small business checklist
For organisations
PDF (183.09K)

What is meant by “lawful”?

This is another term that the Data Protection Act does not define. However, “lawful” refers to statute and to common law, whether criminal or civil. An unlawful act may be committed by a public or private-sector organisation.

If processing personal data involves committing a criminal offence, the processing will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence. Such a duty 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;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations;
- a breach of the Human Rights Act 1998. The Act implements the European Convention on Human Rights which, among other things, gives individuals the right to respect for private and family life, home and correspondence.

However, although processing personal data in breach of copyright (for example) will involve unlawful processing, this does not mean that the ICO will pursue allegations of breach of copyright (or any other law) as this would go beyond the remit of the Data Protection Act. Many areas of law are complex, and the ICO is not and cannot be expected to be expert in all of them.

Principle 2 – purposes

Other sections of this guide explain that you may only process personal data if you have a legitimate basis for doing so, and that any processing must be fair and lawful. This section explains the Data Protection Act's additional requirement that you specify the purpose or purposes for which you obtain personal data, and that anything you do with the data must be compatible with this (or, as the Data Protection Act says, "not … in any manner incompatible" with it.)

In brief – what does the Data Protection Act say about specifying the purposes for which personal data is processed?

The Data Protection Act says that:

> 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.

This requirement (the second data protection principle) aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.

There are clear links with other data protection principles – in particular the first principle, which requires personal data to be processed fairly and lawfully. If you obtain personal data for an unlawful purpose, for example, you will be in breach of both the first data protection principle and this one. However, if you comply with your obligations under the other data protection principles, you are also likely to comply with this principle, or at least you will not do anything that harms individuals.

In practice, the second data protection principle means that you must:

- be clear from the outset about why you are collecting personal data and what you intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

In more detail…

Why do I need to specify the purpose (or purposes) for which personal data is to

be processed?

You need to be clear about the purpose or purposes for which you hold personal data so that you can then ensure that you process the data in a way that is compatible with your original purpose or purposes (or ”not incompatible”, as the Data Protection Act says.) Specifying those purposes at the outset is likely to help you avoid the possibility of “function creep”. It should also help you decide what information to give individuals to comply with the Act’s fair processing requirements.

How should I specify the relevant purpose (or purposes)?

If you make sure that you process personal data in accordance with the other data protection principles, and that you have notified the Information Commissioner if you need to do so, you are likely to comply with the requirement to “specify” without doing anything more. Nevertheless, the Act says that there are two ways in particular in which you can specify the relevant purposes:

- in a “privacy notice” given to individuals at the time their personal data is collected; or
- in a notification given to the Information Commissioner.

In reality, of course, members of the public do not check your ICO notification entry very often, and you can inform people more effectively by sending them good privacy notices than just by notifying the Information Commissioner. You should also remember that whatever you tell people, and whatever you notify to the Information Commissioner, this cannot make fundamentally unfair processing fair.

Where your organisation is exempt from notification, and processes personal data only for an obvious purpose (and therefore does not need to give a privacy notice), the “specified purpose” should be taken to be the obvious purpose.

Example

A not-for-profit chess club only uses personal data to organise a chess league for its members. The club is exempt from notification, and the purpose for which it processes the information is so obvious that it does not need to give privacy notices to its members. The specified purpose of processing should be taken to be the organisation of a members’ chess league.

Once personal data has been obtained for a specified purpose, can it then be used for other purposes?

The Data Protection Act does not prohibit this, but it does place a limitation on it: the second data protection principle says, in effect, that personal data must not be processed for any purpose that is incompatible with the original purpose or purposes.

When is one purpose compatible with another?

The Act clarifies to some extent what is meant by compatibility – it says that when deciding whether disclosing personal data is compatible with the purpose for which you obtained it, you should bear in mind the purposes for which the information is intended to be used by any person to whom it is disclosed.

An additional or different purpose may still be compatible with the original one. Because it can be difficult to distinguish clearly between purposes that are compatible and those that are not, we focus on whether the intended use of the information complies with the Act's fair processing requirements. It would seem odd to conclude that processing personal data breached the Act on the basis of incompatibility if the organisation was using the information fairly.

If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), you have to consider whether this will be fair. If using or disclosing the information would be unfair because it would be outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, then you should regard the use or disclosure as incompatible with the purpose you obtained the information for.

Example

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

In practice, you often need to get prior consent to use or disclose personal data for a purpose that is additional to, or different from, the purpose you originally obtained it for.

Principle 3 – adequacy

The Data Protection Act requires you to ensure you only collect the personal data you need for the purposes you have specified. You are also required to ensure that the personal data you collect is sufficient for the purpose for which it was collected.

These requirements of data adequacy and data minimisation are covered by principle 3 of the Data Protection Act. It is the first of three principles, along with principles 4 and 5, covering information standards.

In brief – what does the Data Protection Act say about the amount of personal data you may hold?

The Act says that:

> Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

This is the third data protection principle. In practice, it means you should ensure that:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
- you do not hold more information than you need for that purpose.

So you should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information, but no more. This is part of the practice known as "data minimisation".

In more detail...

What is meant by "adequate, relevant and not excessive"?

The Data Protection Act does not define these words. Clearly, though, they need to be considered:

- in the context of the purpose for which you are holding the personal data; and
- separately for each individual you hold information about (or for each group of individuals where the individuals in the group share relevant characteristics).

So, to assess whether you are holding the right amount of personal data, you must first be clear about why you are holding and using it. You should take into account that this may differ from one individual to

another.

When is an organisation holding too much personal data?

You should not hold more personal data than you need. Nor should the data you hold include irrelevant details.

Example

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The agency should delete most of their personal data, keeping only the minimum data needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

Where sensitive personal data is concerned, it is particularly important to make sure you collect or retain only the minimum amount of information you need.

If you need to hold particular information about certain individuals only, you should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people.

Example

A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job.

Example

An employer holds details of the blood groups of all its employees. Some of them do hazardous work and the information is needed in case of accident. For the rest of the workforce, though, such information is likely to be irrelevant and excessive.

You should not hold personal data on the off-chance that it might be useful in the future. However, it is permissible to hold information for a foreseeable event that may never occur, as in the above example about blood groups.

When is an organisation holding insufficient personal data?

Personal data should not be processed if it is insufficient for its intended purpose.

Example

A CCTV system is installed to identify individuals entering and leaving a building. However, the quality of the CCTV images is so poor that identification is difficult. This undermines the purpose for which the CCTV system was installed.

In some circumstances you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question.

Example

A group of individuals set up a club. At the outset the club has only a handful of members, who all know each other, and the club's activities are administered using only basic information about the members' names and email addresses. The club proves to be very popular and its membership grows rapidly. It becomes necessary to collect additional information about members so that the club can identify them properly, and so that it can keep track of their membership status, subscription payments etc.

What about the adequacy and relevance of opinions?

The Data Protection Act does not give individuals the right to demand that you delete an opinion about them from your records because they believe it is based on irrelevant information, or has not taken account of information they think is important. However, the record of an opinion (or of the context it is held in) should contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position. If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, this should be made clear.

Example

A GP's record may hold only a letter from a consultant and it will be the hospital file that contains greater detail. In this case, the record of the consultant's opinion should contain enough information to enable the more detailed records to be traced.

For information about the accuracy of opinions, see Keeping personal data accurate and up to date.

Principle 4 – accuracy

The second of the principles covering information standards, principle 4 covers the accuracy of personal data. The Data Protection Act imposes obligations on you to ensure the accuracy of the personal data you process. It must also be kept up to date where necessary.

This requirement is closely linked with the requirement under principle 3 that personal data is adequate. Ensuring the accuracy of personal data will assist you in complying with this requirement as well.

In brief – what does the Data Protection Act say about accuracy and updating?

The Act says that:

> Personal data shall be accurate and, where necessary, kept up to date.

This is the fourth data protection principle. Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. So the Act makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

To comply with these provisions you should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

In more detail...

- When is personal data "accurate" or "inaccurate"?
- What about records of mistakes?
- Does personal data always have to be up to date?
- How does the general rule that information must be accurate apply to information I compile?
- What about information individuals provide, or which I obtain from third parties?
- What are "reasonable steps"?
- What happens when individuals challenge the accuracy of information?
- What about the accuracy of opinions?

When is personal data "accurate" or "inaccurate"?

The Data Protection Act does not define the word "accurate", but it does say that personal data is inaccurate if it is incorrect or misleading as to any matter of fact. It will usually be obvious whether information is accurate or not. For example, if an individual has moved house from Chester to Wilmslow, a record showing that he currently lives in Chester is obviously inaccurate. But a record showing that he once lived in Chester remains accurate, even though he no longer lives there. You must always be clear about what a record is intended to show.

Example

A journalist builds up a profile of a particular public figure. This includes information derived from rumours circulating on the internet that the individual was once arrested on suspicion of dangerous driving. If the journalist records that the individual was arrested, without qualifying this, he or she is asserting this as an accurate fact. However, if it is clear that the journalist is recording rumours, the record is accurate – the journalist is not asserting that the individual was arrested for this offence.

Example

The Post Office Address File (PAF) contains UK property postal addresses. It is structured to reflect the way the Royal Mail delivers post. So it is common for someone to have a postal address linked to a town in one county (eg Stoke-on-Trent in Staffordshire) even if they actually live in another county (eg Cheshire) and pay council tax to that council. The PAF file is not intended to accurately reflect county boundaries.

What about records of mistakes?

There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably don't want their records to be tarnished by, for example, a penalty or other charge that was later cancelled or refunded. However, the organisation may legitimately wish its records to accurately reflect what actually happened – in this example, that a charge was imposed, and later cancelled or refunded. Keeping a record of a mistake and its correction might also be in the individual's interests.

Example

A mis-diagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis because it is relevant for the purpose of explaining treatment given to the patient, or to additional health problems.

It is acceptable to keep records of events that happened in error, provided those records are not misleading about the facts. You may need to add a note to a record to clarify that a mistake happened.

Example

An individual finds that, because of an error, their account with their existing energy supplier has been closed and an account opened with a new supplier. Understandably aggrieved, they believe the original account should be reinstated and no record kept of the unauthorised transfer. Although this reaction is understandable, if their existing supplier did close their account, and another supplier opened a new account, then records reflecting what actually happened will be accurate. In such cases it makes sense to ensure that the record clearly shows that an error occurred.

Example

An individual is dismissed for alleged misconduct. An Employment Tribunal finds that the dismissal was unfair and the individual is reinstated. The individual demands that the employer deletes all references to misconduct. However, the record of the dismissal is accurate. The Tribunal's decision was that the employee should not have been dismissed on those grounds. The employer should ensure its records reflect this.

Does personal data always have to be up to date?

This depends on what the information is used for. If the information is used for a purpose that relies on it remaining current, it should be kept up to date. For example, your employee payroll records should be updated when there is a pay rise. Similarly, records should be updated for customers' changes of address so that goods are delivered to the correct location.

In other circumstances, it will be equally obvious when information does not need to be updated.

Example

An individual places a one-off order with an organisation. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

Also, where information is held only for statistical, historical or other research reasons, updating the information might even defeat the purpose of holding it.

How does the general rule that information must be accurate apply to information I compile?

Where you use your own resources to compile personal data about an individual, then you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual. If, for example, you give an employee a pay increase on the basis of an annual increment and a performance bonus, then there is no excuse for getting the new salary figure wrong in your payroll records.

The exception to the rule – what does the Act say about information individuals provide about themselves, or which I obtain from third parties?

It may be impractical to check the accuracy of personal data someone else provides. In recognition of this, the Act says that even if you are holding inaccurate personal data, you will not be considered to have breached the fourth data protection principle as long as:

- you have accurately recorded information provided by the individual concerned, or by another individual or organisation;
- you have taken reasonable steps in the circumstances to ensure the accuracy of the information; and
- if the individual has challenged the accuracy of the information, this is clear to those accessing it.

What are “reasonable steps”?

This will depend on the circumstances and, in particular, the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you will be using the data in making decisions that may significantly affect the individual concerned or others, you will need to put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the data is accurate. For example, most employers will only need to check the precise details of job applicants’ education, qualifications and work experience if it is essential for that particular role, when they would need to obtain authoritative verification.

Example

An organisation recruiting a driver will want proof that the individuals they interview are entitled to drive the type of vehicle involved. The fact that an applicant states in his work history that he worked as a Father Christmas in a department store 20 years ago will not need to be checked for this particular job.

If your information source is someone you know to be reliable, or is a well-known organisation, it will usually be reasonable to assume that they have given you accurate information. However, in some circumstances you will need to double-check – for example if inaccurate information could have serious consequences, or if common sense suggests there may be a mistake.

Example

A business that is closing down recommends a member of staff to another organisation. Assuming the two employers know each other, it may be reasonable for the organisation to which the recommendation is made to accept assurances about the individual's work experience at face value. However, if a particular skill or qualification is needed for the new job role, the organisation would need to make appropriate checks.

Example

An individual sends an email to her mobile phone company requesting that it changes its records about her willingness to receive marketing material. The company amends its records accordingly without making any checks. However, when the customer emails again asking the company to send her bills to a new address, they carry out additional security checks before making the requested change.

What happens when individuals challenge the accuracy of information held about them?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it. Sometimes the individual may be able to provide convincing documentary evidence that, for example, a date of birth has been recorded incorrectly. In other circumstances, you may need to make some checks yourself.

Example

When an individual tells a credit reference agency its record of a particular account is wrong, the agency will usually have to contact the lender concerned to confirm that the record is accurate. If the lender satisfies the credit reference agency that the record is correct then the agency can retain it. However, if the agency is not satisfied that the record is accurate, it should amend or remove it. The credit reference agency will mark the record as being in dispute while the lender looks into the matter but it must tell the individual whether it has amended or removed the record within 28 days of receiving the challenge.

Where the accuracy of a record has been challenged by the individual it relates to, it is good practice to mark the record as being in dispute (as in the above example). You are not legally obliged to do this – so, if you are satisfied that a record is correct, you need not flag it as having been challenged. However,

in the case of credit reference agency records, it is accepted industry practice that disputed information should be flagged. In any event, the advantage of flagging a disputed record is that (as long as the other conditions are satisfied) it avoids you breaching the fourth data protection principle if the information does turn out to be inaccurate.

If an individual is not satisfied that you have taken appropriate action to keep their personal data accurate, they may apply to the court for an order that you rectify, block, erase or destroy the inaccurate information.

For more information, see:

> Correcting inaccurate personal data
> For organisations

What about the accuracy of opinions?

We have already considered the adequacy of opinions, but questions also arise as to the accuracy of an opinion.

An expression of an opinion about an individual is classed as their personal data. Two people may have very different opinions about the ability or personality of an individual. Personal experiences and preferences, even prejudices, can colour a person's opinions, so it may be impossible to conclude with any confidence which, if either, of two conflicting opinions is accurate. People may only be able to state which of the two they tend to agree with. So when recording information about an individual, you should record whether it is an opinion, and, where appropriate, whose opinion it is.

Some records that may appear to be opinions do not contain an opinion at all. For example, many financial institutions use credit scores to help them decide whether to provide credit. A credit score is a number that summarises the historical credit information on a credit report and provides a numerical predictor of the risk involved in granting an individual credit. Credit scores are based on a statistical analysis of individuals' personal data, rather than on a subjective opinion about their creditworthiness.

An area of particular sensitivity is medical opinion, where doctors routinely record their opinions about possible diagnoses. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (or informed opinion) may prove to be incorrect after more extensive examination or further tests. Individuals sometimes want the initial diagnosis to be deleted on the grounds that it was, or proved to be, inaccurate. However, if the patient's records accurately reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect a particular doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later.

How much weight is placed on an opinion is likely to depend on the experience and reliability of the person whose opinion it is, and what they base their opinion on. An opinion formed during a brief meeting will probably be given less weight than one derived from considerable dealings with the individual. The "adequacy" requirement is relevant in these cases (see The amount of personal data you may hold).

If a court is satisfied that you are holding inaccurate personal data containing an expression of opinion that appears to the court to be based on that inaccurate data, it can order you to delete all of that data, including the expression of opinion.

Principle 5 – retention

The last of the three information standards principles, principle 5 requires you to retain personal data no longer than is necessary for the purpose you obtained it for. This principle has close links with both principles 3 and 4. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.

This section answers some common questions about how long personal data should be kept. It sets out briefly the duties of organisations in this regard, and gives examples of good practice in managing the retention of personal data.

In brief – what does the Data Protection Act say about keeping personal data?

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This is the fifth data protection principle. In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

In more detail...

- Why should I worry about retaining personal data?
- What approach should I take to decisions about retaining personal data?
- What determines the length of a retention period?
- What the information is used for
- The surrounding circumstances
- Any legal or regulatory requirements
- Agreed industry practices
- What should happen to personal data at the end of its retention period?
- What about keeping shared information?

Why should I worry about retaining personal data?

Assuming that you have a good reason for processing the personal data in question, it is obvious that discarding that data too soon would be likely to disadvantage your business and, quite possibly, to

inconvenience the people the information is about as well. However, keeping personal data for too long may cause the following problems:

- There is an increased risk that the information will go out of date, and that outdated information will be used in error – to the detriment of all concerned.
- As time passes it becomes more difficult to ensure that information is accurate.
- Even though you may no longer need the personal data, you must still make sure it is held securely.
- You must also be willing and able to respond to subject access requests for any personal data you hold. This may be more difficult if you are holding more data than you need.

We have already mentioned the links between the third, fourth and fifth data protection principles. So, for example, personal data held for longer than necessary will, by definition, be excessive and may also be irrelevant. In any event, it is inefficient to hold more information than necessary.

What approach should I take to decisions about retaining personal data?

It is good practice to regularly review the personal data you hold, and delete anything you no longer need. Information that does not need to be accessed regularly, but which still needs to be retained, should be safely archived or put offline.

If you hold more than small amounts of personal data, it is good practice to establish standard retention periods for different categories of information. You will need to take account of any professional rules or regulatory requirements that apply. It is also advisable to have a system for ensuring that your organisation keeps to these retention periods in practice, and for documenting and reviewing the retention policy. For example, if any records are not being used, you should reconsider whether they need be retained.

If you only hold a modest amount of personal data, you may not need a formal data retention policy. You must still comply with the law, of course, so it is good practice to conduct a regular audit, and to check through the records you hold to make sure you are not holding onto personal data for too long, or deleting it prematurely.

What determines the length of a retention period?

Personal data will need to be retained for longer in some cases than in others. How long you retain different categories of personal data should be based on individual business needs. A judgement must be made about:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure it remains accurate and up to date.

The appropriate retention period is also likely to depend on the following.

What the information is used for

How long you should keep personal data depends on the purpose for which it was obtained and its nature. If it continues to be necessary to hold the data for one of the reasons set out in Schedules 2 and 3 of the Data Protection Act (such as the performance of a public function or compliance with employment law), then you should retain it for as long as that reason applies. On the other hand, information with only a short-term value may have to be deleted within days.

Example

A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank. Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons.

Example

Images from a CCTV system installed to prevent fraud at an ATM machine may need to be retained for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, images from a CCTV system in a pub may only need to be retained for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the images will need to be retained until the police have time to collect them.

Where personal data is held for more than one purpose, there is no need to delete the data while it is still needed for any of those purposes. However, personal data should not be kept indefinitely "just in case", or if there is only a small possibility that it will be used.

Example

A tracing agency holds personal data about a debtor so that it can find that individual on behalf of a creditor. Once it has found the individual and reported to the creditor, there may be no need to retain the information about the debtor – it should be removed from the agency's systems unless there are good reasons for keeping it. Such reasons could include if the agency has also been asked to collect the debt, or because the agency is authorised to use the information to trace debtors on behalf of other creditors.

There may often be good grounds for keeping personal data for historical, statistical or research purposes. The Data Protection Act provides that personal data held for these purposes may be kept indefinitely as long as it is not used in connection with decisions affecting particular individuals, or in a way that is likely to cause damage or distress. This does not mean that the information may be kept

forever – it should be deleted when it is no longer needed for historical, statistical or research purposes.

The surrounding circumstances

If personal data has been recorded because of a relationship between you and the individual, you should consider whether you need to keep the information once the relationship ends.

Example

The individual may be a customer who no longer does business with you. When the relationship ends, you must decide what personal data to retain and what to delete.

You may not need to delete all personal data when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.

Example

In the previous example, you may need to keep some personal data about the customer so that you can deal with any complaints they might make about the services you provided.

Example

An employer should review the personal data it holds about an individual when that individual leaves the organisation's employment. It will need to retain enough data to enable the organisation to deal with, say, providing references or information about the individual's pension arrangements. However, personal data that is unlikely to be needed again should be removed from the organisation's records – such as the individual's emergency contact details, previous addresses, or death-in-service beneficiary details.

Example

A business receives a notice from a former customer requiring it to stop processing the customer's personal data for direct marketing. It is appropriate for the business to retain enough information about the former customer for it to stop including that person in future direct marketing activities.

In some cases, you may need to keep personal data so you can defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

Example

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

Any legal or regulatory requirements

There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If an organisation keeps personal data to comply with a requirement like this, it will not be considered to have kept the information for longer than necessary.

Agreed industry practices

How long certain kinds of personal data should be kept may also be governed by specific business-sector requirements and agreed practices. For example, we have agreed that credit reference agencies are permitted to keep consumer credit data for six years.

What should happen to personal data at the end of its retention period?

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful where many records of the same type are held.

However, there is a significant difference between permanently deleting a record and archiving it. If a record is archived or stored offline, this should reduce its availability and the risk of misuse or mistake. However, you should only archive a record (rather than delete it) if you still need to hold it. You must be

prepared to give subject access to it, and to comply with the data protection principles. If it is appropriate to delete a record from a live system, it should also be deleted from any back-up of the information on that system.

The word ‘deletion’ can mean different things in relation to electronic data. We have produced detailed guidance which sets out how organisations can ensure compliance with the DPA, in particular the fifth data protection principle, when archiving or deleting personal information:

> Deleting personal data
> For organisations
> PDF (257.46K)

What about keeping shared information?

Where personal data is shared between organisations, those organisations should agree about what to do once they no longer need to share the information. In some cases, it may be best to return the shared information to the organisation that supplied it, without keeping a copy. In other cases, all the organisations involved should delete their copies of the information.

Example

Personal data about the customers of Company A is shared with Company B, which is negotiating to buy Company A’s business. The companies arrange for Company B to keep the information confidential, and use it only in connection with the proposed transaction. The sale does not go ahead and Company B returns the customer information to Company A without keeping a copy.

The organisations involved in an information-sharing initiative may need to set their own retention periods, because some may have good reasons to retain personal data for longer than others. However, if shared information should be deleted, for example because it is no longer relevant to the initiative, then all the organisations with copies of the information should delete it.

Principle 6 – rights

The Data Protection Act gives rights to individuals in respect of the personal data that organisations hold about them. The Act says that:

> Personal data shall be processed in accordance with the rights of data subjects under this Act.

This is the sixth data protection principle, and the rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

This part of the guide explains these rights, sets out the duties of organisations in this regard and gives examples of good practice.

Subject access request

In brief – what is an individual entitled to?

This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret). Other rights relating to these types of decisions are dealt with in more detail in Automated decision taking.

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request. For more information, please see Exemptions.

> Subject access checklist
> For organisations

In more detail...

- What is an individual entitled to?
- What is a valid subject access request?
- Can I require individuals to use a form?
- Can I send out an old version of the data?
- Do I have to explain the content?
- Can I charge a fee?
- Can I ask for more information before responding?
- What about requests made on behalf of others?
- What about requests for information about children?
- What should I do if the data includes information about other people?
- What about data held by credit reference agencies?

- What if I use a data processor?
- What if it's time consuming or expensive?
- What about repeat or unreasonable requests?
- Can I require an individual to make a subject access request?

What is an individual entitled to?

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. So it is important to establish whether the information requested falls within the definition of personal data. In most cases, it will be obvious whether the information being requested is personal data, but we have produced separate guidance to help you decide in cases where it is unclear: Determining what is personal data (pdf). Please also see the key definitions.

Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

Various exemptions from the right of subject access apply in certain circumstances or to certain types of personal data; see Exemptions.

What is a valid subject access request?

For a subject access request to be valid, it should be made in writing. You should also note the following points when considering validity:

- A request sent by email or fax is as valid as one sent in hard copy. Requests may also be validly made by means of social media; please refer to the Subject access code of practice (pdf) for guidance on this.
- You do not need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so (as long as you are satisfied about the person's identity), and it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them.
- If a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, you may have to make a reasonable adjustment for them under the Equality Act 2010 (in Northern Ireland this falls under the Disability Discrimination Act 1995). This could include treating a verbal request for information as though it were a valid subject access request. You might also have to respond in a particular format which is accessible to the disabled person, such as Braille, large print, email or audio formats. If an individual thinks you have failed to make a reasonable adjustment, they may make a claim under the Equality Act (or Disability Discrimination Act 1995 in Northern Ireland). Information about making a claim is available from the Equality and Human Rights Commission or, as appropriate, from the Equality Commission for Northern Ireland.
- If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that you and your colleagues can recognise a subject

access request and treat it appropriately.

Can I require individuals to use a specially designed form when making subject access requests?

No. Many organisations produce subject access request forms, and you may invite individuals to use such a form as long as you make it clear that this is not compulsory and you do not try to use this as a way of extending the 40-day time limit for responding. Standard forms can make it easier for you to recognise a subject access request and make it easier for the individual to include all the details you might need to locate the information they want.

However, any request in writing must be considered as a valid request, whatever the format.

I have received a request but need to amend the data before sending out the response. Should I send out the "old" version?

The Act specifies that a subject access request relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So it would be reasonable for you to supply information you hold when you send out a response, even if this is different to that held when you received the request.

However, it is not acceptable to amend or delete the data if you would not otherwise have done so. For organisations subject to Freedom of Information legislation, it is an offence to make such an amendment with the intention of preventing its disclosure.

Do I have to explain the contents of the information I send to the individual?

The Act requires that the information you provide to the individual is in "intelligible form". At its most basic, this means that the information you provide should be capable of being understood by the average person. However, the Act does not require you to ensure that the information is provided in a form that is intelligible to the particular individual making the request.

Example

An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as "A", while non-attendance at a similar event is logged as "M". Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to the organisation's key or index to explain this information, it would be impossible for anyone outside the organisation to understand. In this case, the Act requires you to explain the meaning of the coded information. However, although it would be good practice to do so, the Act does not require you to decipher the poorly written notes, since the meaning of "intelligible form" does not extend to "make legible".

Example

You receive a subject access request from someone whose English comprehension skills are quite poor. You send a response and they ask you to translate the information you sent them. The Act does not require you to do this since the information is in intelligible form, even if the person who receives it cannot understand all of it. However, it would be good practice for you to help them understand the information you hold about them.

Can I charge a fee for dealing with a subject access request?

Yes, an organisation receiving a subject access request may charge a fee for dealing with it, except in certain circumstances relating to health records. If you choose to charge a fee, you need not comply with the request until you have received the fee. The usual maximum fee you can charge is £10. There are different fee arrangements for organisations that hold credit, health or education records. Please refer to the Subject access code of practice (pdf) for more details, and for credit reference agencies please also see What about personal data held by credit agencies?

Although you need not comply with a request until you have received a fee, you cannot ignore a request simply because the individual has not sent a fee. If a fee is payable but has not been sent with the request, you should contact the individual promptly and inform them that they need to pay.

Some organisations choose not to charge a fee. However, once you have started dealing with an individual's request without asking for a fee, it would be unfair to then demand a fee as a way of extending the period of time you have to respond to the request.

Can I ask for more information before responding to a subject access request?

The Act allows you to confirm two things before you are obliged to respond to a request.

First, you can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.

The key point is that you must be reasonable about what you ask for. You should not request lots more information if the identity of the person making the request is obvious to you. This is particularly the case, for example, when you have an ongoing relationship with the individual.

Example

You have received a written subject access request from a current employee. You know this employee personally and have even had a phone conversation with them about the request. Although your organisation's policy is to verify identity by asking for a copy of a utility bill, it would be unreasonable to do so in this case since you know the person making the request.

However, you should not assume that, on every occasion, the person making a request is who they say they are. In some cases, it is reasonable to ask the person making the request to verify their identity before sending them information.

Example

An online retailer receives a subject access request by email from a customer. The customer has not used the site for some time and although the email address matches the company's records, the postal address given by the customer does not. In this situation, it would be reasonable to gather further information, which could be as simple as asking the customer to confirm other account details such as a customer reference number, before responding to the request.

The level of checks you should make may well depend on the possible harm and distress which inappropriate disclosure of the information could cause to the individual concerned.

Example

A GP practice receives a subject access request from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requestor is the patient to whom the record relates. In this situation, it would be reasonable for the practice to ask for more information before responding to the request. The potential risk to the former patient of sending their health records to the wrong person is such that the practice is right to be cautious. They could ask the requestor to provide more information, such as a date of birth, a passport or a birth certificate.

The second thing you are entitled to do before responding to a subject access request is to ask for information that you reasonably need to find the personal data covered by the request. Again, you need not comply with the subject access request until you have received this information. In some cases, personal data may be difficult to retrieve and collate. However, it is not acceptable for you to delay responding to a subject access request unless you reasonably require more information to help you find the data in question.

Example

A chain of supermarkets is dealing with a general subject access request from a member of staff at one of their branches. The person dealing with the request is satisfied that the staff member has been sent all information held in personnel files and in files held by his line manager. However, he complains that not all information about him was included in the response. The employer should not ignore this complaint, but it would be reasonable to ask the member of staff for further details. For example, some of the information may be in emails, and the employer could reasonably ask for the dates when the emails were sent, and who sent them, to help find the information requested.

It might also be useful for the employer to ask if the member of staff is seeking information that does not relate to his employment. For example, he may be seeking information that relates to a complaint he made as a customer of the supermarket.

As with a request that is sent without the required fee, you should not ignore a request simply because you need more information from the person who made it. You should not delay in asking for this, but should ensure the individual knows you need more information and should tell them what details you need. Provided you have done so, the 40-day period for responding to the request does not begin to run until you have received the appropriate fee and any additional information that is necessary.

What about subject access requests made on behalf of others?

The Act does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Example

A building society has an elderly customer who visits a particular branch to make weekly withdrawals from one of her accounts. Over the past few years, she has always been accompanied by her daughter who is also a customer of the branch. The daughter makes a subject access request on behalf of her mother and explains that her mother does not feel up to making the request herself as she does not understand the ins and outs of data protection. As the information held by the building society is mostly financial, it is rightly cautious about giving customer information to a third party. If the daughter had a general power of attorney, the society would be happy to comply. They ask the daughter whether she has such a power, but she does not.

Bearing in mind that the branch staff know the daughter and have some knowledge of the relationship she has with her mother, they might consider complying with the request by making a voluntary disclosure. However, the building society is not obliged to do so, and it would not be unreasonable to require more formal authority.

If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the Data Protection Act, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters:

- in England and Wales, by the Court of Protection;
- in Scotland, by the Sheriff Court; and
- in Northern Ireland, by the High Court (Office of Care and Protection).

What about requests for information about children?

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, for example, to a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than a parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a subject access request. The presumption does not apply in England and Wales or in Northern Ireland, but it does indicate an approach that will be reasonable in many cases. It does not follow that, just because a child has capacity to make a subject access request, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so.

What should I do if the data includes information about other people?

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The Act says you do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

For the avoidance of doubt, you cannot refuse to provide subject access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

Please refer to the Subject access code of practice (pdf) for more information.

For further information, read our more detailed guidance:

How to disclose information safely – removing personal data from information requests and datasets

For organisations
PDF (1.31MB)

What about personal data held by credit reference agencies?

There are special provisions regulating access to personal data held by credit reference agencies. Where credit reference agencies hold personal data relevant to an individual's financial standing (information in a credit reference file), they must provide a copy of the information within seven days of a written request and on payment of a £2 fee. Credit reference agencies will need to verify the identity of the person making the request before they respond.

Read more about information held by credit reference agencies:

Credit explained
For the public
PDF (889.45K)

If I use a data processor, does this mean they would have to deal with any subject access requests I receive?

Responsibility for complying with a subject access request lies with you as the data controller. The Act does not allow any extension to the 40-day time limit in cases where you have to rely on a data processor to provide the information that you need to respond.

Example

An employer is reviewing staffing and pay, which involves collecting information from and about a representative sample of staff. A third-party data processor is analysing the information.

The employer receives a subject access request from a member of staff. To respond, the employer needs information held by the data processor. The employer is the data controller for this information and should instruct the data processor to retrieve any personal data that relates to the member of staff.

If you use a data processor, then you need to make sure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the data processor.

Read an explanation of the role of a data processor in Who has rights and obligations under the Data Protection Act?

What if sending out copies of information will be expensive or time consuming?

In some cases, dealing with a subject access request will be an onerous task. This might be because of

the nature of the request, because of the amount of personal data involved, or because of the way in which certain information is held.

Under section 8(2) of the Act you are not obliged to supply a copy of the information in permanent form if it would involve disproportionate effort to do so. You must decide whether supplying a copy of the information would involve disproportionate effort. Even if you do not have to supply a copy of the information in permanent form, the individual still has the other basic rights described above.

The Act does not define "disproportionate effort" but it is clear that there is some (albeit limited) scope for assessing whether complying with a request would result in so much work or expense as to outweigh the individual's right of access to their personal data. However, it should be noted that this qualification to the right of subject access only applies in respect of "supplying" a copy of the relevant information in permanent form. So you cannot refuse to deal with a subject access request just because you think that locating the information in the first place would involve disproportionate effort.

Please refer to the Subject access code of practice (pdf) for more details on this provision.

We stress that you should rely on this provision only in the most exceptional of cases. The right of subject access is central to data protection law and we rarely hear of instances where an organisation could legitimately use disproportionate effort as a reason for not allowing an individual to access their personal data. Even if you can show that supplying a copy of information in permanent form would involve disproportionate effort, you should still try to comply with the request in some other way.

Example

An organisation has decided that to supply copies of an individual's records in permanent form would involve disproportionate effort. Rather than refuse the individual access, they speak to her and agree that it would be preferable if she visited their premises and viewed the original documents. They also agree that if there are documents that she would like to take away with her, they can arrange to provide copies.

What about repeated or unreasonable requests?

The Data Protection Act does not limit the number of subject access requests an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Act says that you are not obliged to comply with an identical or similar request to one you have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

The Act gives you some help in deciding whether requests are made at reasonable intervals. It says that you should consider the following:

- the nature of the data – this could include considering whether it is particularly sensitive;
- the purposes of the processing – this could include whether the processing is likely to cause detriment to the individual; and
- how often the data is altered – if information is unlikely to have changed between requests, you may

decide that you are not obliged to respond to the same request twice.

If there has been a previous request or requests, and the information has been added to or amended since then, you might consider whether you need only provide the new or updated information to the requester. However section 8(6) of the Act states that "information to be supplied pursuant to a request….must be supplied by reference to the data in question at the time when the request is received…". This means that, when answering a SAR, you are required by the Act to provide a full response to the request: not merely providing information that is new or has been amended since the last request.

In practice we would accept that you may attempt to negotiate with the requester to get them to restrict the scope of their SAR to the new or updated information; however, if the requester insists upon a full response then you would need to supply all the information.

Example

A library receives a subject access request from an individual who made a similar request one month earlier. The information relates to when the individual joined the library and the items borrowed. None of the information has changed since the previous request. With this in mind, along with the fact that the individual is unlikely to suffer if no personal data is sent in response to the request, the library need not comply with this request. However, it would be good practice to respond explaining why they have not provided the information again.

Example

A therapist who offers non-medical counselling receives a subject access request from a client. She had responded to a similar request from the same client three weeks earlier. When considering whether the requests have been made at unreasonable intervals, the therapist should take into account the fact that the client has attended five sessions between requests, so there is a lot of new information in the file. She should respond to this request (and she could ask the client to agree that she only needs to send any "new" information). If the client does not agree, the therapist should provide a copy of all the information on the file.

But it would also be good practice to discuss with the client a different way of allowing the client access to the notes about the sessions.



Subject access code of practice

Practical advice on what to do if you get a request from an individual for personal information.

Subject access code of practice (Welsh language) (pdf)

Can I require an individual to make a subject access request?

It is a criminal offence, in certain circumstances and in relation to certain information, to require an individual to make a subject access request.

For more information on enforced subject access requests:

Enforced subject access requests (section 56)
For organisations
PDF (259.75K)

Further reading

Access Assist - free iPad app from Allen & Overy (iTunes)
External link

Access to information held in complaint files
For organisations
PDF (142.64K)

Subject access checklist
For organisations

> PDF (141.3K)

Damage or distress

In brief – what does the Data Protection Act say about objecting to processing?

The Act refers to the "right to prevent processing". Although this may give the impression that an individual can simply demand that an organisation stops processing personal data about them, or stops processing it in a particular way, the right is often overstated. In practice, it is much more limited. An individual has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question.

So, in certain limited circumstances, you must comply with such a requirement. In other circumstances, you must only explain to the individual why you do not have to do so.

In more detail...

How can an individual prevent me processing their personal data?

An individual who wants to exercise this right has to put their objection in writing to you and state what they require you to do to avoid causing damage or distress. We refer to this notice as an "objection to processing" although it is also known as a "section 10 notice" in practice. The Act limits the extent to which you must comply with such an objection, in the following ways:

- an individual can only object to you processing their own personal data;
- processing an individual's personal data must be causing unwarranted and substantial damage or distress; and
- the objection must specify why the processing has this effect.

In addition, an individual has no right to object to processing if:

- they have consented to the processing;
- the processing is necessary:
  - in relation to a contract that 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 (other than a contractual obligation); or
- the processing is necessary to protect the individual's "vital interests".

Example

A mobile phone company receives a written request from a customer requiring it to remove the customer's details from its database. This should be treated as an objection to processing. The customer explains that using their personal data for credit referencing is causing them distress and has led to them being refused a credit card. The mobile phone company does not have to comply with this notice because the credit referencing is necessary for putting into effect the contract that the customer signed (and the customer can be said to have consented to it). Consequently, the right to object to processing does not apply. It would be good practice for the mobile phone company to write to the customer to explain why it does not have to comply with the notice.

Example

The same customer cancels his mobile phone contract and withdraws his consent to the company processing his personal data. As a result he argues that the mobile phone company must comply with his objection. Although the right to object does now apply (because the mobile phone company cannot rely on any of the conditions for processing), the company only has to comply with the objection (ie to stop processing the customer's personal data) if the processing is causing unwarranted and substantial damage or distress. The company must, however, respond to the customer within 21 days, explaining whether and to what extent it will comply with the objection.

In its response, the mobile phone company accepts that being refused a credit card might be considered financially damaging, but says that the effect on the customer is not unwarranted, since sharing information about the customer's payment history with the agencies is justified and because the customer had been informed in advance that this would happen. The company is therefore entitled to refuse to comply with the notice.

The individual's right to object to processing only extends to their own personal data, so they cannot prevent the processing of personal data relating to another individual or group of individuals. Nevertheless, an individual may still issue an objection to processing on behalf of another person.

What is meant by "damage or distress"?

The Act does not define what is meant by unwarranted and substantial damage or distress. However, in most cases:

- substantial damage would be financial loss or physical harm; and
- substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent.

Example

An individual is refused a job in the construction industry and discovers that this is because the prospective employer checked his name against a blacklist maintained by a third party. The blacklist consists of the names of people who are regarded as unsuitable to be employed in the construction industry because they are trade union activists. The individual writes to the person who maintains the blacklist asking them to remove his name as it is denying him the opportunity to gain employment.

In these circumstances, the person who maintains the blacklist would have great difficulty in establishing any legitimate basis for processing the individual's personal data in this way – because the assessment of "unsuitability" is arbitrary and lacks justification, and because the individuals concerned were not told that their names had been placed on the blacklist. In any event, the individual can show that he is suffering damage due to this processing and that this is substantial as it could continue to prevent him getting a job. It cannot be argued that the damage was warranted, because the processing was for an improper purpose. The person who maintains the blacklist would therefore have to comply with the objection. He must cease processing the individual's personal data in this way, and must respond to the objection within 21 days confirming that he has done so.

The Act recognises that organisations may have legitimate reasons for keeping records about people which may have a "negative" effect on them. For example, the information you hold may lead to their arrest, to their being made to pay child maintenance, or to their being required to buy a TV licence. The Act does not give individuals the right to prevent this. Even where damage or distress has been caused, the Act limits the right to prevent processing to cases where the effects are unwarranted.

Example

An individual writes to his local council asking them to stop using his personal data for administering and collecting Council Tax. Despite his argument that the processing is financially damaging and very irritating, it is clear that the cost to the individual is not unwarranted and that his annoyance at having to pay does not constitute substantial distress.

Any objection to processing must be based on a causal link between the processing of personal data and the damage or distress caused to the individual – the processing must have caused the damage or distress.

Example

A bank files a default with a credit reference agency because Customer A has failed to repay a personal loan. Due to an administrative error, the default is filed against Customer B, who has a similar name to Customer A but has no liability in respect of the personal loan. If the record of the default causes Customer B to be refused credit when he would otherwise have been granted credit, the bank's incorrect processing of his personal data has clearly caused damage.

How should I respond to an objection to processing?

An objection to processing will tell you what the individual wants you to do. So you need to decide whether you will comply with their request. The Act allows room for a decision that is more nuanced than simply “yes, we will comply" or “no, we do not have to comply”.

Example

An employee discovers that his electronic HR file contains a negative comment about his political allegiances and resulting suitability for promotion. He writes to his employer demanding that it stops processing his personal data. The employer is entitled to respond that it will delete the reference to the individual’s political allegiances and any associated remarks, but that it intends to continue processing his personal data for legitimate HR purposes.

Example

An employer is investigating allegations of harassment against one of its employees. The employee in question emails the HR department demanding that the investigation is discontinued and that any notes about it are destroyed. The employer is entitled to refuse to comply with this request because it has legitimate reasons to keep a record of the investigation, but it can agree to add a note to the file recording the employee’s insistence that the allegations are untrue.

There are several factors you should take into account when deciding whether and to what extent you intend to comply with an objection to processing. These factors are listed in the table below.

Factors to check	Points to note
Is the objection to processing in writing?	An objection is valid only if it is in writing. Like subject access requests, “in writing” includes information sent by fax or email. Once you receive a written objection, you have 21 calendar days to respond to the individual who sent it.
Does the objection set out how the processing is causing damage or distress?	It is difficult to decide whether to comply with an objection to processing if the notice is unclear. You may wish to ask the individual who sent it to clarify what they think is the problem that processing their personal data has caused. Remember that the damage or distress caused has to be “substantial” before you are obliged to comply.
Is the damage or distress unwarranted?	If you feel that any damage or distress caused to the individual is warranted, you do not have to comply with the objection. You should be prepared to explain why you think this is the case.

Which conditions for processing can you rely on to legitimise the processing?	If you can rely on any of the first four conditions listed in Schedule 2 to the Act, the individual has no right to prevent the processing in question, and you do not have to comply with an objection. You must still send a response.

You must respond within 21 days of receiving the objection to processing. Your response must state what you intend to do and, if you do not intend to comply with the objection in some way, give reasons for your decision. Your record of the decisions you made about the factors listed above will help you compose your response.

What happens if I do not comply with an objection to processing?

If you decide that an objection to processing is not justified and you do not comply with it, the individual can apply to the court. The court can decide whether the objection is justified and, if necessary, order you to take steps to comply.

Preventing direct marketing

In brief – what does the Data Protection Act say about direct marketing?

Individuals have the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give you written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if you receive a notice you must comply within a reasonable period.

For more information, read our direct marketing guidance (pdf) (and direct marketing checklist (pdf)).

In more detail...

- What is direct marketing?
- Should I respond to a notice to stop direct marketing?
- When an individual sends a notice, should I delete their details?
- Do I have to suppress details immediately?
- Do I have any other duties when using personal data?
- Can I ask people if they want to opt back in?
- What about the Mailing Preference Service?
- Does the same apply to the Telephone Preference Service?
- What about electronic marketing?

What is direct marketing?

The Act includes some help on what is meant by "direct marketing" in a data protection context. The table below sets out the factors that are used to identify direct marketing material.

Directed to particular individuals	Lots of people receive "junk mail" that is not addressed to a particular person but to "the occupier". This type of marketing is not directed at an individual and so is not direct marketing for the purposes of the Act. This kind of mail, posted through every letterbox on a street, includes leaflets like takeaway menus and information about clothing collections.
Communication by whatever means	The common image of direct marketing is that of mailshots or telemarketing. However, for the purposes of the Act it also includes all other means by which you might contact individuals, such as emails and text messages.

Advertising or marketing material	Direct marketing does not just refer to selling products or services to individuals. It includes promoting particular views or campaigns, such as those of a political party or charity. So, even if you are using personal data to elicit support for a good cause rather than to sell goods, you are still carrying out direct marketing and would have to comply with a written notice to stop.

So you must stop any promotional activity directed at a particular individual, using that person's personal data to communicate the promotional activity to them, if they write and ask you to stop.

Should I respond to a notice to stop direct marketing?

The Act does not require that you respond to a notice to stop direct marketing – it only requires you to stop. This is because you have no discretion about whether to comply with such a notice. However, acknowledging that you have received and acted on a notice is good practice, where this is appropriate.

When an individual sends a notice, should I delete their details?

Individuals will often ask you to remove or delete their details from your database or marketing list. However, in most cases it is preferable to follow the marketing industry practice of suppressing their details. Rather than deleting an individual's details entirely, suppression involves retaining just enough information about them to ensure that their preferences are respected in future. Suppression allows you to ensure that you do not send marketing to people who have asked you not to, and means that you have a record against which you can check any new marketing lists. If you delete people's details, you have no way of ensuring that they are not put back on your database. Deleting an individual's details may also breach industry-specific legal requirements about how long you should hold personal data.

Do I have to suppress details immediately?

The Act says that you should stop processing for direct marketing purposes within a reasonable period. When considering whether you have done so, we take into account that a particular marketing campaign might already be underway when you receive a notice, and that the individual may subsequently receive further marketing material. However, we expect that in normal circumstances electronic communications should stop within 28 days of receiving the notice, and postal communications should stop within two months.

Do I have any other duties when using personal data for direct marketing?

You must comply with the data protection principles, including the duty to process personal data fairly. In the context of direct marketing, this will involve making sure that the people whose information you are using are aware that they may receive marketing material from you. You might also consider whether you plan to pass your marketing lists to other organisations and how you will be contacting people, such as by post, phone, or email.

It is important to remember that the right to prevent the use of personal data for direct marketing purposes is a kind of "opt-out". So you could market people until they send written notice telling you not to. However, if you fail to deal properly with a notice (perhaps due to a technical difficulty), an individual could apply to the court and the court could order you to comply with the notice. You should make every effort to avoid this, so it is good practice to give an individual the opportunity to object to future contact at the time you collect personal data from them, such as during a phone call or on a website, or when they sign an application form for a product or service. You can also use this opportunity to find out how they would like to be contacted.

Can I ask people if they want to opt back in to receiving direct marketing?

If an individual has asked you to stop using their details for direct marketing purposes, they did so deliberately. You should not assume that they did so lightly or are happy to receive requests to change their mind. A notice to stop direct marketing applies to sending direct marketing material and also to processing personal data for direct marketing. In other words, the notice the individual gave you is likely to cover using their personal data to persuade them to allow you to put them back on your marketing list, and so you should avoid asking.

However, we recognise that people can change their minds and that marketing techniques also change. There is some merit in making sure the preferences people have previously expressed are up to date, but you should do this sensitively and should certainly avoid doing anything that could mean an individual has to inform you that their preferences have not changed.

Example

A fitness centre regularly mails a newsletter to its members. Some members have objected to this use of their personal data and the fitness centre has, quite properly, flagged this objection on their system.

The fitness centre wants to ensure that these previously expressed wishes have not changed, particularly since the content of the newsletter has changed considerably over the last few months and it can also now be sent out as an email. They cannot assume that people may have changed their minds and it would be good practice to assume that any objections they received recently are still an accurate reflection of the members' wishes.

For "older" objections, they could mention the changes to the newsletter and the possibility of receiving it by email in any "usual course of business" contact they have with the member, such as a membership renewal letter, but they should not contact the members concerned with the specific intention of showing them "what they are missing".

We consider that it is acceptable to remind individuals of their ability to change their marketing preferences if the reminder forms a minor and incidental addition to a message you are sending them anyway.

Example

A bank sends out annual statements to its customers detailing transactions on their deposit accounts during the previous year. A message is printed at the bottom of each statement to remind customers that they may wish to review their marketing preferences and telling them how to update them.

What about the Mailing Preference Service?

When sending direct marketing by post, it is good practice to screen your mailing lists against the lists held by the Mailing Preference Service (MPS). Individuals can register with MPS to reduce the amount of direct marketing mail they receive. Although marketers have no legal duty to check the MPS before sending direct marketing, many reputable organisations do so.

Does the same apply to the Telephone Preference Service?

No. There are legally enforceable rules which prevent you making telesales calls to any subscriber who has told you to stop making such calls to their number. In addition, subscribers can register with the Telephone Preference Service (TPS) to prevent unsolicited telesales calls. You cannot make or instigate the making of unsolicited telesales calls to any number listed on the TPS register. Registration with the TPS does not override specific consents which an individual has given to particular organisations. Read about how to comply with the rules about telesales:

Direct marketing
For organisations
PDF (507.67K)

What about electronic marketing?

Telephone marketing is regarded as a form of electronic marketing. Marketing which is conducted this way, or is sent by other electronic means (by fax, email, or text message) is subject to extra rules set out in the Privacy and Electronic Communications (EC Directive) Regulations 2003. We have published a separate guide that explains how to comply with these rules:



Guide to privacy and electronic communications

This guide explains your obligations under the Regulations and answers many frequently asked questions.

Automated decision taking

In brief – what does the Data Protection Act say about automated decision taking?

The right of subject access allows an individual access to information about the reasoning behind any decisions taken by automated means. The Act complements this provision by including rights that relate to automated decision taking. Consequently:

- an individual can give written notice requiring you not to take any automated decisions using their personal data;
- even if they have not given notice, an individual should be informed when such a decision has been taken; and
- an individual can ask you to reconsider a decision taken by automated means.

These rights can be seen as safeguards against the risk that a potentially damaging decision is taken without human intervention. We explain below what is meant by automated decision taking and how the rights work in practice.

The number of organisations who take significant decisions about individuals by wholly automated means is relatively small – there is often some human intervention in making the decisions. However, it is sensible to identify whether any of the operations you perform on personal data constitute "automated decisions". This will help you decide whether you need to have procedures to deal with the rights of individuals in these cases.

In more detail...

When do the rights arise (what is an automated decision)?

The rights in respect of automated decisions only arise if two requirements are met. First, the decision has to be taken using personal data processed solely by automatic means.

Example

An individual applies for a personal loan online. The website uses algorithms and auto credit searching to provide an immediate yes/no decision on the application.

Example

A factory worker's pay is linked to his productivity, which is monitored automatically. The decision about how much pay the worker receives for each shift he works is made automatically by reference to the data collected about his productivity.

So the rights explained here do not apply to any decision involving human intervention. Many decisions that are commonly regarded as "automated" actually involve human intervention.

Example

An employee is issued with a warning about late attendance at work. The warning was issued because the employer's automated clocking-in system flagged the fact that the employee had been late on a defined number of occasions. However, although the warning was issued on the basis of the data collected by the automated system, the decision to issue it was taken by the employer's HR manager following a review of that data. So the decision was not taken by automated means.

The second requirement is that the decision has to have a significant effect on the individual concerned.

Example

In the above example on monitoring the productivity of a factory worker, it is obvious that a decision about how much pay he is entitled to will have a significant effect on him.

So these rights do not apply to decisions that only affect the individual to a trivial or negligible extent.

Example

An individual enters an online "personality quiz". She answers questions about herself on a website, which uses her responses to automatically generate a personality profile for her. The individual's data is not retained and the profile is not sent to anyone else. The automated decisions on which the personality profile is based do not have a significant effect on the individual.

Are all automated decisions subject to these rights?

No. Some decisions are called "exempt decisions" because the rights do not apply, even though they are taken using solely automated means and do significantly affect the individual concerned.

Exempt decisions:

are authorised or required by legislation; **OR**

are taken in preparation for, or in relation to, a contract with the individual concerned

AND

are to give the individual something they have asked for; **OR**

are where steps have been taken to safeguard the legitimate interests of the individual, such as allowing them to appeal the decision.

What rights do individuals have?

The Act gives individuals three rights in relation to automated decision taking.

The first is the right to prevent such a decision being taken. You must not take an automated decision if an individual has given notice in writing asking you not to.

The second right applies where no such notice has been given. An organisation that takes an automated decision must inform the individual concerned that it has done this. It must do so as soon as is practicable in the circumstances.

The third right relates to the options available to an individual on receiving this information. If an individual is unhappy that an automated decision has been taken, they have 21 days to ask you to reconsider the decision or to take a new decision on a different basis. In most cases, both these options are likely to involve a review of the automated decision.

Example

An individual complains to a credit provider because his online application for credit was declined automatically. The application was declined because the information provided by the individual did not match pre-defined acceptance criteria applied by the automated system. The credit provider undertakes manual underwriting checks to review the original decision.

If a court is satisfied that you have failed to comply with these rights, it may order you to do so.

Correcting inaccurate personal data

In brief – what does the Data Protection Act say about rights to correct or delete inaccurate information?

The fourth data protection principle requires personal data to be accurate (see Keeping personal data accurate and up to date). Where it is inaccurate, the individual concerned has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. In addition, where an individual has suffered damage in circumstances that would result in compensation being awarded and there is a substantial risk of another breach, then the court may make a similar order in respect of the personal data in question.

In more detail...

What if the inaccurate information was received from the individual concerned or from a third party?

It may be impractical to check the accuracy of personal data someone else provides. In recognition of this, the Act says that even if you are holding inaccurate personal data, you will not be considered to have breached the fourth data protection principle as long as:

- you have accurately recorded information provided by the individual concerned, or by another individual or organisation;
- you have taken reasonable steps in the circumstances to ensure the accuracy of the information (see Keeping personal data accurate and up to date and Retaining personal data); and
- if the individual has challenged the accuracy of the information, this is clear to those accessing it.

In these circumstances the court may (as an alternative to ordering the rectification etc. of the inaccurate data) order that a statement of the true facts (in terms approved by the court) should be added to the record that contains it. And, if the court is not satisfied that you complied with the above requirements, it may order you to do so.

Example

A couple who have a seriously ill baby object to the contents of their child's hospital records, saying they are inaccurate. Some of the information they object to came from the baby's health visitor. Having tried without success to resolve the dispute informally, they go to court to ask for the records to be amended.

The court could order the hospital to rectify, block, erase, or destroy any inaccurate personal data. To the extent that the inaccurate data was provided by the health visitor, the court could (as an alternative) order that the data be supplemented by a statement of the true facts.

What about opinions based on inaccurate personal data?

This right also applies to personal data that contain an expression of opinion based on inaccurate personal data.

Example

In the example above, the child's parents claim that one of the reasons the hospital's records are inaccurate is that they include a doctor's opinion which is based on the inaccurate information provided by the health visitor. If it agrees, the court may order that the statement of opinion be rectified, blocked, erased or destroyed. Alternatively, it may order that the statement of opinion be supplemented by a statement recording that it was based on inaccurate information.

Should other people be told when inaccurate information is corrected or deleted?

If a court has ordered you to rectify, block, erase or destroy personal data, then it can also order you to notify any third parties to whom you have disclosed the information. The court would probably only require this if it is reasonable to expect that you would be able to comply with the order. As a matter of good practice, we would expect you to take reasonable steps to do this whether or not the court requires you to do so.

Example

A bank is ordered to correct inaccurate information about an individual's liability to repay a loan. The bank routinely provides information about such matters to the credit reference agencies. The court may order the bank to inform the credit reference agencies that the information has been

corrected – and the bank should do so in any event.

Compensation

In 2015 the Court of Appeal ruled, in the case of Vidal-Hall v Google, that compensation under the DPA could be awarded for distress alone, however this aspect of the judgment has been appealed by Google and will now be heard by the Supreme Court. The ICO will review this guidance once the Supreme Court has issued its judgment.

In brief – what does the Data Protection Act say about the right to compensation?

If an individual suffers damage because you have breached the Act, they are entitled to claim compensation from you. This right can only be enforced through the courts. The Act allows you to defend a claim for compensation on the basis that you took all reasonable care in the circumstances to avoid the breach.

In more detail...

Does the Act define "damage"?

No. But an individual who has suffered financial loss because of a breach of the Act is likely to be entitled to compensation.

Example

A customer of an internet mail order company has been the subject of a security breach. All his information, including his credit card details, was freely available on the internet for almost 24 hours before the site was taken down. He has had to freeze his credit card account and is worried that he will be a victim of identity fraud.

He does not trust the company not to do this again. They had been the cause of a previous security breach, and at that time he had asked to have his details removed from their customer list. He asks the court to award him compensation. The court may do so if the individual can show that he has suffered financial loss because of the breach of the Act.

What about distress?

In many cases, a breach of the Act will not cause an individual financial loss, but it may be distressing to find that personal data has been processed improperly. If an individual has suffered damage, any compensation awarded may take into account the level of any associated distress, but distress alone will not usually be sufficient to entitle an individual to compensation (unless the processing was for the purposes of journalism, literature or art).

Example

An individual's name is entered onto an employee fraud database without justification. The individual is understandably distressed to discover the implication that he is a fraudster. However, the information about him is removed from the database before he applies for a new job, and so he suffers no damage as a result of the error. The employee has no entitlement to compensation for distress alone.

Example

In the previous example, the fact that the individual's name appears on the fraud database prevents him from obtaining a job he has applied for. He suffers financial damage as a result. He is entitled to claim compensation for this damage and for the distress he has suffered as well.

What level of compensation might be involved?

There are no guidelines about levels of compensation in this area. Often, the parties can reach agreement about the amount of compensation which is appropriate. If they cannot agree, the court will have to decide. If an individual claims a certain amount in compensation, they will need to be able to show how your failure to comply with the Act has resulted in their incurring that amount of loss or damage.

The ICO cannot award compensation, or give advice on the appropriate level of compensation, even where we have made an assessment that an organisation is likely to have breached the Act.

Can you defend a claim for compensation?

You can obviously defend a claim if you have not breached the Act. If there has been a breach, you can still defend a claim for compensation, but only if you can show that you took such care as was reasonably required in the circumstances to comply with the Act. What you will have to prove will depend on the nature of the breach in question. What is reasonable will depend on the circumstances.

In data protection terms, this means that you have looked at the way you process and protect personal data and that you put in place appropriate checks to prevent any problems occurring. Your defence may rely on describing these checks. Some form of positive action is often necessary and, if a reasonable step or precaution has not been taken, then the defence is likely to fail.

Principle 7 – security

This part of the guide offers an overview of what the Data Protection Act requires in terms of security, and aims to help you decide how to manage the security of the personal data you hold. We cannot provide a complete guide to all aspects of security in all circumstances and for all organisations, but this part identifies the main points. We also provide details of other sources of advice and information about security.

There is no "one size fits all" solution to information security. The security measures that are appropriate for an organisation will depend on its circumstances, so you should adopt a risk-based approach to deciding what level of security you need.

In brief – what does the Data Protection Act say about information security?

The Data Protection Act says that:

> 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.

This is the seventh data protection principle. In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- be clear about who in your organisation is responsible for ensuring information security;
- make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

In more detail...

- Why should I worry about information security?
- What needs to be protected by information security arrangements?
- What level of security is required?
- What kind of security measures might be appropriate?
- What is the position when a data processor is involved?
- What should I do if there is a security breach?
- What other sources of information and advice are there?

Why should I worry about information security?

Information security breaches may cause real harm and distress to the individuals they affect – lives may even be put at risk. Examples of the harm caused by the loss or abuse of personal data (sometimes linked to identity fraud) include:

- fake credit card transactions;
- witnesses at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and women at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Not all security breaches have such grave consequences, of course. Many cause less serious embarrassment or inconvenience to the individuals concerned. Individuals are entitled to be protected from this kind of harm as well.

Advances in technology have enabled organisations to process more and more personal data, and to share information more easily. This has obvious benefits if they are collecting and sharing personal data in accordance with the data protection principles, but it also gives rise to equally obvious security risks. The more databases that are set up and the more information that is exchanged, the greater the risk that the information will be lost, corrupted or misused.

A number of high-profile losses of large amounts of personal data have brought attention to the issue of information security. However, these incidents have also made it clear that information security is an issue of public concern as well as technical compliance. If personal data is not properly safeguarded, this can seriously damage an organisation’s reputation and prosperity and can compromise the safety of individuals.

What needs to be protected by information security arrangements?

It is important to understand that the requirements of the Data Protection Act go beyond the way information is stored or transmitted. The seventh data protection principle relates to the security of every aspect of your processing of personal data.

So the security measures you put in place should seek to ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

What level of security is required?

The Act says you should have security that is appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

The Act does not define "appropriate". But it does say that an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved. The Act does not require you to have state-of-the-art security technology to protect the personal data you hold, but you should regularly review your security arrangements as technology advances. As we have said, there is no "one size fits all" solution to information security, and the level of security you choose should depend on the risks to your organisation.

So, before deciding what information security measures you need to take, you will need to assess your information risk: you should review the personal data you hold and the way you use it to assess how valuable, sensitive or confidential it is, and what damage or distress could be caused to individuals if there were a security breach.

Example

An organisation holds highly sensitive or confidential personal data (such as information about individuals' health or finances) which could cause damage or distress to those individuals if it fell into the hands of others. The organisation's information security measures should focus on any potential threat to the information or to the organisation's information systems.

This risk assessment should take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have;
- the extent of their access to the personal data; and
- personal data held or used by a third party on your behalf (under the Data Protection Act you are responsible for ensuring that any data processor you employ also has appropriate security).

What kind of security measures might be appropriate?

The Data Protection Act does not define the security measures you should have in place. However, particular security requirements that apply within particular industries may impose certain standards or require specific measures. In general terms, which security measures are appropriate will depend on your circumstances, but there are several areas you should focus on. Physical and technological security is likely to be essential, but is unlikely to be sufficient of itself. Management and organisational security measures are likely to be equally important in protecting personal data.

Management and organisational measures

Carrying out an information risk assessment is an example of an organisational security measure, but you will probably need other management and organisational measures as well. You should aim to build a culture of security and awareness within your organisation.

Perhaps most importantly, it is good practice to identify a person or department in your organisation with day-to-day responsibility for security measures. They should have the necessary authority and resources to fulfil this responsibility effectively.

Example

The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that the organisation has appropriate information security measures, and to make regular reports on security to the organisation's board. The Resources department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

Unless there is clear accountability in your organisation for such security measures, they will probably be overlooked and your organisation's overall security will quickly become flawed and out of date.

Not every organisation will need a formal information security policy – this will depend on things like the size of the organisation, the amount and nature of the personal data it holds, and the way it uses the data. Whether or not these matters are written into a formal policy, all organisations will need to be clear about them, and about related matters such as the following:

- co-ordination between key people in the organisation (for example, the security manager will need to know about commissioning and disposing of any IT equipment);
- access to premises or equipment given to anyone outside the organisation (for example, for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how to protect and recover any personal data the organisation holds; and
- periodic checks to ensure that the organisation's security measures remain appropriate and up to date.

Staff

It is vital that your staff understand the importance of protecting personal data; that they are familiar with your organisation's security policy; and that they put its security procedures into practice. So you must provide appropriate initial and refresher training, and this should cover:

- your organisation's duties under the Data Protection Act and restrictions on the use of personal data;
- the responsibilities of individual staff members for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;
- the proper procedures to use to identify callers;
- the dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making "phishing" attacks) or by persuading you to alter information when you should not do so; and
- any restrictions your organisation places on the personal use of its computers by staff (to avoid, for

example, virus infection or spam).

The effectiveness of staff training is dependent on the individuals concerned being reliable in the first place. The Data Protection Act requires you to take reasonable steps to ensure the reliability of any staff who have access to personal data.

Example

An organisation verifies the identity of its employees when they are recruited by asking to see passports or driving licences before they start work. It also obtains appropriate references to confirm their reliability. The organisation's standard contract of employment sets out what staff can and cannot do with the personal data they have access to.

Physical security

Technical security measures to protect computerised information are of obvious importance. However, many security incidents relate to the theft or loss of equipment, or to old computers or hard-copy records being abandoned.

Physical security includes things like the quality of doors and locks, and whether premises are protected by alarms, security lighting or CCTV. However, it also includes how you control access to premises, supervise visitors, dispose of paper waste, and keep portable equipment secure.

Example

As part of its security measures, an organisation ensures that information on laptop computers issued to staff is protected by encryption, and that desk-top computer screens in its offices are positioned so that they cannot be viewed by casual passers-by. Paper waste is collected in secure bins and is shredded on site at the end of each week.

Computer security

Computer security is constantly evolving, and is a complex technical area. Depending on how sophisticated your systems are and the technical expertise of your staff, you may need specialist information-security advice that goes beyond the scope of this guide. A list of helpful sources of information about security is provided at the end of this chapter. You should consider the following guiding principles when deciding the more technical side of information security.

- Your computer security needs to be appropriate to the size and use of your organisation's systems.
- As noted above, you should take into account technological developments, but you are also entitled to consider costs when deciding what security measures to take.

- Your security measures must be appropriate to your business practices. For example, if you have staff who work from home, you should put measures in place to ensure that this does not compromise security.
- The measures you take must be appropriate to the nature of the personal data you hold and to the harm that could result from a security breach.

For further information, see our IT security top tips or read our more detailed guidance:

- IT asset disposal for organisations (pdf) – Guidance to help organisations securely dispose of old computers and other IT equipment; and
- A practical guide to IT security: ideal for the small business (pdf)
- Bring your own device (BYOD) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data that they are responsible for.
- Guidance on the use of cloud computing (pdf) – this guidance covers how the security requirements of the DPA apply to personal data processed in the cloud.
- Encryption – Advice on the use of encryption to protect personal data.

What is the position when a data processor is involved?

Organisations may use third party data processors to process personal data on their behalf (see Key definitions of the Data Protection Act – Who has rights and obligations under the Data Protection Act?) for the definition of this term). This often causes security problems. Particular care is needed because the organisation (and not the data processor) will be held responsible under the Data Protection Act for what the data processor does with the personal data.

The Act contains special provisions that apply in these circumstances. It says that, where you use a data processor:

- you must choose a data processor that provides sufficient guarantees about its security measures to protect the processing it will do for you;
- you must take reasonable steps to check that those security measures are being put into practice; and
- there must be a written contract setting out what the data processor is allowed to do with the personal data. The contract must also require the data processor to take the same security measures you would have to take if you were processing the data yourself. A model data processing contract has been published by the European Committee for Standardization.

What should I do if there is a security breach?

If, despite the security measures you take to protect the personal data you hold, a breach of security occurs, it is important that you deal with the security breach effectively. The breach may arise from a theft, a deliberate attack on your systems, from the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure. However the breach occurs, you must respond to and manage the incident appropriately. Having a policy on dealing with information security breaches is another example of an organisational security measure you may have to take to comply with the seventh data protection principle.

There are four important elements to any breach-management plan:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.

4. Evaluation and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly.

These issues are considered in greater detail in our guidance on data security breach management (pdf). We have also produced Notification of data security breaches to the ICO (pdf) and Notification of PECR security breaches (pdf). These provide guidance on:

- the circumstances in which we expect organisations to notify us of security breaches;
- the information we need in those circumstances; and
- what organisations can expect us to do after they notify us.

Use our security breach notification form (Word) to report a breach to us.

What other sources of information and advice are there?

General advice

> Department for Business Innovation and Skills
> External link

> The Cyber Essentials scheme
> External link

There is an international standard for information security management:

A detailed look at ISO 27001; includes an audit and certification scheme

> ISO website - ISO/IEC 27001
> External link

BSI Group website - ISO/IEC 27001
External link

Principle 8 – international

This section provides practical advice to companies or other organisations who want to send personal data outside the European Economic Area (EEA).

In brief – what does the Data Protection Act say about sending personal data outside the EEA?

The Data Protection Act says that:

> Personal data shall not be transferred to a country or territory outside the EEA 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.

This is the eighth data protection principle, but other principles of the Act will also usually be relevant to sending personal data overseas. For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas. The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using sub-contractors abroad.

The Act also sets out the situations where the eighth principle does not apply, and these situations are also considered in more detail in this section.

If you are considering sending personal data outside the EEA, work through the following checklist to help you decide if the eighth principle applies and, if so, how to comply with it to make a transfer.

1. Do you need to transfer personal data abroad?

Can you achieve your objectives without processing personal data at all? For example, could the information be anonymised?

2. Are you transferring the data to a country outside the EEA or will it just be in transit through a non-EEA country?

If data is only in transit through a non-EEA country, there is no transfer outside the EEA. Note that if you add personal data to a website based in the EU that is accessed in a country outside the EEA, there will be a transfer of data outside the EEA.

3. Have you complied with all the other data protection principles?

If you transfer personal data outside the EEA, you are required to comply with all the principles and the Act as a whole, not just the eighth principle relating to international data transfers.

4. Is the transfer to a country outside the EEA?

There are no restrictions on the transfer of personal data to EEA countries.

5. Is the transfer to a country on the EU Commission's list of countries or territories providing adequate protection for the rights and freedoms of data subjects in connection with the processing of their personal data?

Transfers may be made to any country or territory in respect of which the Commission has made a 'positive finding of adequacy'.

6. If the transfer is to the United States of America, has the US recipient of the data provided adequate protection for the transfer of personal data?

For the latest information on the transfer of personal data to the USA please see our blog, Safe Harbor: calmer waters on the horizon.

7. Is the personal data passenger name record information (PNR)?

The agreement made between the EU and the USA (to legitimise and regulate the transfer of PNR from EU Airlines to the US Department of Homeland Security) is regarded as providing adequate protection for the rights of the data subjects whose personal data (in the form of PNR) is transferred. Arrangements also exist between the European Commission, Canada and Australia.

If you decide you need to transfer personal data outside the EEA, and the recipient is not in a country subject to a Commission 'positive finding of adequacy' nor signed up to the Safe Harbor Scheme, you will need to assess whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects in connection with the transfer/processing of their personal data.

8. Can you make an assessment that the level of protection for data subjects' rights is 'adequate in all the circumstances of the case'?

> Assessing adequacy for international data transfers
> For organisations
> PDF (205.41K)

9. If not, can you put in place adequate safeguards to protect the rights of the data subjects whose data is to be transferred?

Adequate safeguards may be put in place in a number of ways including using Model Contract Clauses, Binding Corporate Rules or Binding Corporate Rules for Processors (BCRs) or other contractual arrangements. Where "adequate safeguards" are established, the rights of data subjects continue to be protected even after their data has been transferred outside the EEA.

10. Can you rely on another exception from the restriction on international transfers of personal data?

Schedule 4 DPA concerns "Cases where the Eighth Principle does not apply". It covers BCRs, model contract clauses, and the use of other contractual clauses as well as a number of other exceptions to the restriction on overseas data transfers. If you are able to rely on an exception, the transfer may take place even though there is no other protection for individuals' rights.

In more detail...

- Is it possible to fulfil my objectives and send information outside the UK without processing personal data?
- What is the difference between a transfer and being in transit?
- What other data protection obligations must I comply with when transferring personal data outside the EEA?
- Which countries are in the EEA?
- Which countries have an adequate level of protection?
- If the data protection law in a country has not been approved as adequate, is it still possible to send personal data to that country?
- How do I assess adequacy?
- How can you use contracts to ensure there is an adequate level of protection?
- In what circumstances will the Information Commissioner approve transfers by an organisation?
- What are "binding corporate rules"?
- Are there any exceptions to the rule?
- Can I transfer personal data overseas if I get a request for it from the authorities outside the UK on the basis of the laws in their country?
- What other sources of information and advice are there?

Is it possible to fulfil my objectives and send information outside the UK without processing personal data?

Before making a transfer, you should consider whether you can achieve your aims without actually processing personal data. For example, if data is made anonymous so that it will never be possible to identify individuals from it on its own or by combining it with other available information, the information will not be personal data, the data protection principles will not apply, and you are free to transfer the information outside the EEA.

What is the difference between a transfer and being in transit?

A transfer involves sending personal data to someone in another country.

Example

A company in the UK uses a centralised human resources system in the United States belonging to its parent company to store information about its employees.

Example

A travel agent sends a customer's details to a hotel in Australia where they will be staying while on holiday.

A transfer of personal data for the purposes of the eighth principle occurs when information moves from an EEA country to a country or territory outside the EEA (a third country).

A transfer is not the same as the transit of personal data through a third country. The eighth principle will only apply if the personal data moves to a third country, rather than passing through it on the way to its destination.

Example

Personal data is transferred from country "A" to country "B" via a server in country "C", which does not access or manipulate the information while it is in country "C". In these circumstances the transfer is only to country "B".

You will be processing personal data in the UK and transferring it even if:

you collect information relating to individuals on paper, which is not ordered or structured in any way; and

you send this overseas with the intention that, once it is there, it will be processed using equipment operating automatically; or

it will be added to a highly structured filing system relating to individuals.

Example

A large insurance broker sends a set of notes about individual customers to a company acting on their behalf in another country. These notes are handwritten and are not held on computer or as part of a relevant filing system in the UK. The notes are to be entered onto a computer in the other country and added to a customer management system.

Putting personal data on a website will often result in transfers to countries outside the EEA. The transfers will take place when someone outside the EEA accesses the website. If you load information onto a server based in the UK so that it can be accessed through a website, you should consider the likelihood that a transfer may take place and whether that would be fair for the individuals concerned. If you intend information on the website to be accessed outside the EEA, then this is a transfer.

What other data protection obligations must I comply with when transferring personal data outside the EEA?

It is important to remember that all the data protection principles apply to overseas transfers of personal data – not just the eighth principle. So you must consider how you will comply with the other principles if you transfer. For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas.

The seventh principle (concerning information security) will also be relevant to how the information is sent and introduces the requirement to have contracts in place when using subcontractors abroad.

Which countries are in the EEA?

Providing you are satisfied that you have complied with the other provisions (and in particular the principles) of the DPA, there are no additional restrictions on the transfer of personal data to EEA countries.

The EEA countries are currently the EU countries plus Iceland, Liechtenstein and Norway:

Austria	Germany	Malta
Belgium	Greece	Netherlands
Bulgaria	Hungary	Norway
Croatia	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	Liechtenstein	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
		United Kingdom

Which countries have an adequate level of protection?

The European Commission has decided that certain countries have an adequate level of protection for personal data. Currently, the following countries are considered as having adequate protection.

Andorra	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Canada	Israel	Uruguay

Faroe Islands	Jersey

View an up to date list of such countries on the European Commission's data protection website.

Although the United States of America (USA) is not included in the European Commission list, a Decision of the European Commission in 2000 found that the US-EU "Safe Harbor" framework provided adequate protection for personal data transferred from the EU to US companies that are members of Safe Harbor. Under the Safe Harbor framework US member companies agree to:

- follow seven principles of information handling; and
- be held responsible for keeping to those principles by the Federal Trade Commission or other oversight schemes.

On 6 October 2015 the Court of Justice of the European Union (CJEU) issued a judgment which invalidated the Decision of the European Commission. For further details of the implications of the judgment please read:

> Interim guidance on data transfers to the USA and Safe Harbor
> For organisations
> PDF (111.44K)

In July 2007, the EU and the US signed an agreement to legitimise and regulate the transfer of passenger name record information (PNR) from EU airlines to the US Department of Homeland Security (DHS). This agreement, renewed in 2012, is regarded as providing adequate protection for the personal data in question. There are also agreements on PNR information with Australia and Canada. For more details, please see the European Commission website pages on Passenger Name Record - bilateral agreements.

If the data protection law in a country has not been approved as adequate, is it still possible to send personal data to that country?

Yes, if you are satisfied that in the particular circumstances there is an adequate level of protection. You can:

- assess adequacy yourself;
- use contracts, including the European Commission approved model contractual clauses;
- get your Binding Corporate Rules or Binding Corporate Rules for Processors approved by the Information Commissioner; or
- rely on the exceptions from the rule.

How do I assess adequacy?

You will need to be satisfied that in the particular circumstances there is an adequate level of protection for the rights of the individuals whose personal data you are transferring.

The Act sets out the factors you should take into account in making this decision. This means doing a risk assessment. You must decide whether there is adequate protection for the rights of individuals, in all the circumstances of the transfer. This is known as an assessment of adequacy. To assess adequacy you should look at:

- the nature of the personal data being transferred;
- the country or territory of origin of the information in question;
- the country or territory of final destination of that information;
- how the data will be used and for how long; and
- the security measures to be taken in respect of the personal data in the country or territory where the data will be received.

If your assessment of these 'general adequacy' criteria reveals that, in the particular circumstances, the risks associated with the transfer are low, an exhaustive analysis of the 'legal adequacy' criteria (listed below) may not be necessary. If your assessment of the general adequacy criteria indicates the transfer is 'high risk' (eg if the data is particularly sensitive), then a more comprehensive investigation of the legal adequacy criteria will be required. In these circumstances you must consider:

- the extent to which the country has adopted data protection standards in its law;
- whether there is a way to make sure the standards are achieved in practice; (for example, whether there are any enforceable codes or conduct or other rules); and
- whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

We realise it may be impractical for you to carry out a detailed analysis of adequacy involving the legal situation in a non-EEA country. This analysis might be more appropriate for a business that regularly transfers large volumes of personal data to a particular country, rather than a company that might only occasionally transfer personal data to any of a wide range of countries. For this reason, this guide does not give detailed advice on how to carry out an adequacy test; instead, please see Assessing adequacy for international data transfers (pdf).

In some cases you might reasonably decide there is adequate protection without a detailed assessment. A common situation is where you transfer personal data to a processor acting on your instructions under contract. You are still legally responsible for making sure the data is processed in line with the principles. In particular, personal data can only be transferred if there is a contract requiring the processor to have appropriate security and act only on your instruction. So individuals' information should continue to be protected to the same standard as in the UK and they will have the same rights they can exercise in the UK. This is because you remain liable for ensuring that the processing complies with the data protection principles. When selecting a processor, you need to satisfy yourself that it is reliable and has appropriate security.

However, the level of protection is unlikely to be adequate if:

- the transfer is to a processor in an unstable country; and
- the nature of the information means that it is at particular risk.

For more information see our detailed guidance on Assessing adequacy for international data transfers (pdf) and Outsourcing – a guide for small and medium-sized businesses (pdf).

You may reasonably decide there is adequate protection without a detailed analysis, depending on: the nature of the information; the circumstances of the transfer; your knowledge of the country; and the company you are transferring to. Some examples are discussed below.

Example

A university wishes to transfer the academic biographies of its lecturers and research staff to other universities and potential students outside the EEA. Nothing of a private nature is included.

This is a well-known practice in the university. The personal data, such as the staff's qualifications and publications, is already publicly available. Any member of staff can have their information withheld if they have a reason to do so – such as concerns about their safety. In this case, it is difficult to see a problem with adequacy as the potential for staff to object has been addressed and there is little further risk of misuse.

Example

Company A in the UK sends its customer list to company B outside the EEA so that company B, acting as a processor, can send a mailing to company A's customers. It is likely that adequate protection exists if:

- the information transferred is only names and addresses
- there is nothing particularly sensitive about company A's line of business;
- the names and addresses are for one-time use and must be returned or destroyed within a short timescale;
- company A knows company B is reliable; and
- there is a contract between them governing how the information will be used.

Example

An employee travels outside the EEA with a laptop containing personal data connected with their employment. Their employer in the UK is still the data controller. As long as the information stays with the employee on the laptop, and the employer has an effective procedure to deal with security and the other risks of using laptops (including the extra risks of international travel), it is reasonable to decide that adequate protection exists.

Example

A multinational company transfers a list of internal telephone extensions to its overseas subsidiaries. The nature of the information makes it unlikely that the individuals identified would suffer significant damage in the unlikely event that an unauthorised source obtained the list. It is reasonable to decide that adequate protection exists.

These examples show that you can, in particular circumstances, decide whether there is adequacy. You might limit the types of information you transfer and the types of organisation you transfer to, or insist that the destination company meet certain conditions by contract or otherwise.

If it is not possible to make an assessment that the proposed transfer offers an adequate level of protection, it may be possible to put in place 'adequate safeguards'. Where adequate safeguards are put in place, the rights of individuals continue to be protected even after their data has been transferred outside the EEA. Examples of some of these safeguards are outlined below.

How can you use contracts to ensure there is an adequate level of protection?

There are several types of contract that you can use to transfer personal data outside the EEA. The main types are:

- contracts based on the standard contractual clauses approved by the European Commission (EC model clauses); and
- other contracts you draw up yourself after a risk assessment to bring protection up to an adequate level.

EC model clauses

The European Commission has approved four sets of standard contractual clauses (known as model clauses) as providing an adequate level of protection. If you use these model clauses in their entirety in your contract, you will not have to make your own assessment of adequacy.

Two of the sets of model clauses relate to transferring personal data from one company to another

company, which will then use it for its own purposes (the "controller to controller clauses"). In this case you can choose either set of clauses, depending on which best suits your business arrangements. The other two sets of model clauses are for transferring personal data to a processor acting under your instructions, such as a company that provides you with IT services or runs a call centre for you. Whilst the first set of "processor" model clauses may still be in use for transfer arrangements put in place before 2010, only the new set of "processor" clauses may be used for new arrangements.

The model clauses are attached as an annex to the European Commission decisions of adequacy, which approve their use. The Information Commissioner has authorised the use of both sets of model contracts for transfers from controller to controller: the original 2001 clauses and the revised 2004 clauses. The Information Commissioner has also authorised the use of revised contractual clauses adopted in May 2010 for transfers from controller to processor (pdf), and in doing so has withdrawn his authorisation for the original 2001 clauses for transfers from controller to processor. Contracts made under this authorisation and concluded before 15 May 2010 are still valid. However, the revised clauses should be used from 15 May 2010.

Model contract clauses:

2001 controller to controller
External link

2004 controller to controller
External link

2010 controller to processor
External link

If you are relying on the European Commission adequacy decisions you cannot change the clauses in any way, for example by removing parts or adding other clauses to change the meaning, but the clauses can be incorporated into other contracts. For more information, read our detailed guidance:

Model Contract Clauses: International transfers of personal data.
For organisations
PDF (224.76K)

Other contracts

You can also use your own contracts to help ensure adequacy for a particular transfer or set of transfers. You can use these contracts to plug gaps where you have decided that there would be adequacy, were it not for a particular weakness. For example, you may want to include a contract clause to require the company receiving the information to return it to you if your relationship comes to an end or they go out of business. Alternatively, you may use your own contracts to form the entire basis for the adequacy of protection of individuals' rights.

You do not have to have a separate contract for data protection. You can include the terms to achieve adequacy in any general contract that covers your relationship with the other company.

You can also use contracts where you are not in a position to judge adequacy. The contract should be

comprehensive to enable you to satisfy yourself that adequacy exists, without you needing to analyse the circumstances of the transfer. This kind of contract is likely to be very similar to a standard contract using the EC model clauses, which you can use to develop your own terms.

If you use contract provisions that differ from the model clauses, you risk a future challenge to the adequacy of the contract's level of protection. You must record your reasoning and decisions and be able to justify your actions if you are questioned on them. This is in line with our general approach to compliance with the Act which allows organisations to make their own judgments as to whether they are complying with their data protection obligations rather than always needing to obtain prior approval for their actions. We are not able to give you detailed advice on or approve contracts other than in exceptional circumstances.

In what circumstances will the Information Commissioner approve transfers by an organisation?

The Information Commissioner has the power to authorise transfers of personal data on the basis that in the particular circumstances there is an adequate level of protection, but we will not routinely do this because you will be in a better position to decide if there is adequacy in the light of your knowledge of the safeguards and the processing taking place.

If we authorise a transfer, we must tell the European Commission and other data protection authorities in Europe.

We will not authorise one-off arrangements between you and companies in other countries unless there are exceptional circumstances. We would have to be satisfied that there was no other reasonable way for you to comply with the eighth principle, for example by applying any of the exemptions or by making your own assessment of adequacy.

What are "binding corporate rules"?

Another option is to adopt binding codes of corporate conduct, known as binding corporate rules or binding corporate rules for processors (BCR). This option only applies to multinational organisations transferring information outside the EEA but within their group of entities and subsidiaries. These rules create rights for individuals, which can be exercised before the courts or data protection authorities, and obligations for the company. In all cases, the rules are legally binding on the companies in the multinational group and will usually be made so by unilateral declarations, intra-group agreements or the corporate governance of the group. To use BCR to transfer personal data freely within your group, they must be approved by all the relevant European data protection authorities who will co-operate with each other in assessing the standard of your rules.

You may use internal codes of conduct, similar to BCR, to transfer information from the UK without an authorisation where:

- you have conducted a risk assessment; and
- you are satisfied that the codes provide the level of safeguards required by the eighth principle.

When you do not have an authorisation or your code of conduct or internal policies has not been through the BCR approval process, it will not be recognised as a BCR. Using an unauthorised code risks a future

challenge to the adequacy of the level of protection it offers. If challenged you must be able to justify your reliance on your code of conduct for providing adequate protection. It is therefore important that you record your reasoning and decisions for using your own code. This is in line with our general approach to compliance with the Act.

Read more information on BCR:

Binding corporate rules
For organisations

Are there any exceptions to the rule?

There are several exemptions from the eighth principle, where you can transfer personal data even if there is no adequate protection. However, it is good practice to ensure that there is adequate protection if it is possible to do so, and only to rely on an exemption if it is not. Nevertheless, the exemptions are legally available to you and may in some circumstances provide a simple solution that only results in a minimal loss of protection for the individual. You will find a detailed analysis in our guidance:

The eighth data protection principle and international data transfers
For organisations
PDF (116.49K)

Consent

You can transfer personal data overseas if you have the individual's consent, which should be given clearly and freely and may later be withdrawn by the individual. For further information, see Conditions for processing – What is meant by consent?.

A consent will not be valid if the individual has no choice but to give their consent.

Example

A company asks its employees to agree to the international transfer of their personal data. The penalty for not agreeing is dismissal, and so the company may not rely on any "consents" given by its employees in these circumstances.

The individual must know and have understood what they are agreeing to. You should specify the reasons for the transfer and, as far as possible, the countries involved. If you are aware of any particular risks involved in the transfer, you should tell the individual. In our view, consent is unlikely to provide an adequate long-term solution to repeated transfers or ones that arise from a structural reorganisation.

Contract performance

You can transfer personal data overseas where it is necessary for carrying out certain types of contract or if the transfer is necessary to set up the contract.

For a contract between the organisation and the individual, you may transfer personal data overseas if the transfer is:

- necessary to carry out the contract; or
- a necessary part of the steps the individual has asked you to take before a contract is made between you.

For a contract between the organisation and someone other than the individual, you may transfer personal data overseas if:

- the individual requests the contract or it is in their interests; and
- the transfer is necessary to conclude the contract; or
- the transfer is necessary to carry out such a contract.

In this context, contracts are not restricted to goods and services – they can include employment contracts. Deciding whether a transfer is necessary to carry out a contract depends on the nature of the goods or services provided under the contract rather than how your business is organised.

A transfer is not necessary if the only reason you need to make it is because of the way you have chosen to structure your business. Read more in Conditions for processing.

Example

An individual books a hotel in the USA through a UK travel agent. The UK travel agent will need to transfer the booking details to the USA to fulfil its contract with the individual.

Example

The customer of a UK credit-card issuer uses their card in Japan. It may be necessary for the card issuer to transfer some personal data to Japan to validate the card and/or reimburse the seller.

Example

A UK-based internet trader sells furniture online. It makes it clear to customers that it is a retailer, not a manufacturer. Goods are delivered direct to the customer from the manufacturer. If a customer orders goods that are manufactured in Ukraine, the trader needs to transfer a delivery

name and address to Ukraine to carry out the contract.

Substantial public interest

You can transfer personal data overseas where it is necessary for reasons of substantial public interest. This is a high threshold to meet and it is most likely to be relevant in areas such as preventing and detecting crime; national security; and collecting tax. Organisations intending to rely on this exemption should consider each case individually. The public interest must be that of the UK and not the third country to which the personal data is transferred.

Vital interests

You can transfer personal data overseas where it is necessary to protect the vital interests of the individual. This relates to matters of life and death.

Example

A local health authority could transfer relevant medical records from the UK to another country where an individual had had a heart attack and their medical history was necessary to decide appropriate treatment.

Public registers

You can transfer overseas part of the personal data on a public register, as long as the person you transfer to complies with any restrictions on access to or use of the information in the register.

Example

The General Medical Council (GMC) can transfer extracts from its register of medical practitioners to respond to enquiries from outside the UK, but it is not allowed to transfer the complete register under this exemption. If the GMC puts conditions on inspecting the register in the UK, the person the extract is transferred to, and anyone they then pass it on to, must comply with these restrictions.

Legal claims

You can transfer personal data overseas where it is necessary:

- in connection with any legal proceedings (including future proceedings not yet underway);
- to get legal advice; or
- to establish, exercise or defend legal rights.

Example

A US parent company is sued by an employee of its UK subsidiary. Relevant employee information may be transferred to the US parent as it is required for the defence.

The legal proceedings do not have to involve you or the individual as a party and the legal rights do not have to be yours or the individual's. Although this exemption could apply widely, transfers are only likely to fall under this category if they are connected with legal proceedings or getting legal advice.

Can I transfer personal data overseas if I get a request for it from the authorities outside the UK on the basis of the laws in their country?

No specific exemption routinely covers all such requests. However, in certain circumstances you will be able to send some personal data to the authorities or other parts of your own organisation in another country where the authorities in that country have requested it. How far you may do so will depend on the nature of the request. You will need to consider these cases carefully and you can ask us for advice.

Conditions for processing

This section explains the conditions that need to be satisfied before you may process personal data.

In brief – what does the Data Protection Act say about the "conditions for processing"?

The first data protection principle requires, among other things, that you must be able to satisfy one or more "conditions for processing" in relation to your processing of personal data. Many (but not all) of these conditions relate to the purpose or purposes for which you intend to use the information.

The conditions for processing take account of the nature of the personal data in question. The conditions that need to be met are more exacting when the information being processed is sensitive personal data, such as information about an individual's health or criminal record.

However, our view is that in determining if you have a legitimate reason for processing personal data, the best approach is to focus on whether what you intend to do is fair. If it is, then you are very likely to identify a condition for processing that fits your purpose.

Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately. So it makes sense to ensure that what you want to do with personal data is fair and lawful before worrying about the conditions for processing set out in the Act.

In more detail...

- What are the conditions for processing?
- What is the "legitimate interests" condition?
- What conditions need to be met in respect of sensitive personal data?
- When is processing "necessary"?
- What is meant by "consent"?

What are the conditions for processing?

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual whom the personal data is about has consented to the processing.
- 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.

What is the "legitimate interests" condition?

The Data Protection Act recognises that you may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided you meet certain requirements.

The first requirement is that you must need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it.

Example

A finance company is unable to locate a customer who has stopped making payments under a hire purchase agreement. The customer has moved house without notifying the finance company of his new address. The finance company engages a debt collection agency to find the customer and seek repayment of the debt. It discloses the customer's personal data to the agency for this purpose. Although the customer has not consented to this disclosure, it is made for the purposes of the finance company's legitimate interests – ie to recover the debt.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Example

In the above example, it is clear that the interests of the customer are likely to differ from those of the finance company (it may suit the customer quite well to evade paying his outstanding debt). However, passing his personal data to a debt collection agency in these circumstances could not be called "unwarranted".

Finally, the processing of information under the legitimate interests condition must be fair and lawful and

must comply with all the data protection principles.

Example

Continuing the above example, the finance company must ensure that the personal data it passes to the debt collection agency is accurate (for example, in the known details of the customer's identity); that it is up to date (for example, in the amount outstanding and the customer's last known address); and that it is not excessive – the agency should only get as much personal data as is relevant or necessary for the purpose of finding the customer and recovering the debt.

What conditions need to be met in respect of sensitive personal data?

At least one of the conditions listed above must be met whenever you process personal data. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows.

- The individual whom the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:
  - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual's consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are substantially in the public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration.

A full list of the additional conditions for processing is set out on the legislation.gov website:

> The Data Protection (Processing of Sensitive Personal Data) Order 2000
> External link

When is processing “necessary”?

Many of the conditions for processing depend on the processing being “necessary” for the particular purpose to which the condition relates. This imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.

Example

An employer processes personal data about its employees on the basis that it is necessary to do so in connection with their individual contracts of employment and to comply with the employer’s legal obligations. However, the employer decides to outsource its HR functions to an overseas company and transfers its employees’ data to that company. It is not “necessary” to transfer the data overseas for these purposes, and the employer would instead have to rely on consent, or on the legitimate interests condition, to be able to process its employees’ personal data in this way.

What is meant by “consent”?

One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question.

You will need to examine the circumstances of each case to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent.

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual’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.

The fact that an individual must “signify” their agreement means that there must be some active communication between the parties. An individual may “signify” agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for

example, from a customer’s failure to return a form or respond to a leaflet.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if your organisation intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, you should recognise that the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which you are collecting or using the information. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

You should review whether a consent you have been given remains adequate as your organisation’s relationship with an individual develops, or as the individual’s circumstances change.

Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
- the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be “explicit”.

This suggests that the individual’s consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

As explained above, a particular consent may not be adequate to satisfy the condition for processing (especially if the individual might have had no real choice about giving it), and even a valid consent may be withdrawn in some circumstances. For these reasons an organisation should not rely exclusively on consent to legitimise its processing. In our view it is better to concentrate on making sure that you treat individuals fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data.

Exemptions

In brief – are there any exemptions from the Data Protection Act?

The rights and duties set out in the Data Protection Act are designed to apply generally, but there are some exemptions from the Act to accommodate special circumstances. The exemptions tend to use complex language and, while this chapter has tried to clarify matters, it has had to use some of the same language so as not to mislead.

If an exemption applies, then (depending on the circumstances) you will be exempt from the requirement:

- to register with the ICO (to "notify"); and/or
- to grant subject access to personal data; and/or
- to give privacy notices; and/or
- not to disclose personal data to third parties.

Entitlement to an exemption depends in part on your purpose for processing the personal data in question – for example, there is an exemption from some of the Act's requirements about disclosure and non-disclosure that applies to processing personal data for purposes relating to criminal justice and taxation. However, you must consider each exemption on a case-by-case basis because the exemptions only permit you to depart from the Act's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern.

In more detail...

- What are the exemptions from notification?
- What about exemptions from subject access?
- Disclosure and non-disclosure – how do the exemptions work?
- Disclosure and non-disclosure – when do the exemptions apply?
    - Crime and taxation
    - Regulatory activity
    - Publicly available information
    - Disclosures required by law
    - Legal advice and proceedings
    - Confidential references
    - Management information
    - Negotiations
    - Journalism, literature and art
    - Domestic purposes

- Are there any further exemptions?

What are the exemptions from notification?

Most organisations that process personal data must notify the ICO of certain details about that processing. However, the Act provides exemptions from notification for:

- organisations that process personal data only for:
  - staff administration (including payroll);
  - advertising, marketing and public relations (in connection with their own business activity); and
  - accounts and records;
- some not-for-profit organisations;
- organisations that process personal data only for maintaining a public register;
- organisations that do not process personal information on computer.

Organisations and individuals can use our online self-assessment tool to check whether they need to register with ("notify") the ICO.

What about exemptions from subject access?

We explain in the section of this guidance on subject access requests that an individual has the right to make a request in relation to personal data you hold about them. Several of the exemptions mentioned in the rest of this chapter mean that you do not have to grant subject access in respect of personal data to which the exemption applies.

Also, certain restrictions (similar to exemptions) are built into the Act's subject access provisions. For example, there are restrictions on the disclosure of personal data about more than one individual in response to a subject access request.

Disclosure and non-disclosure – how do the exemptions work?

Different exemptions work in different ways. An exemption may:

- restrict certain rights of individuals in relation to the processing of their personal data; and/or
- limit the duties of organisations when processing that data.

The rights and duties that are affected by one exemption are not necessarily affected by others. So you should look at each exemption carefully to see what effect it has. However, the Act bundles several rights and duties into two groups, and the exemptions tend to work by "disapplying" (blocking) one or both of these groups. The two groups are called the "subject information provisions" and the "non-disclosure provisions".

The subject information provisions are:

- an organisation's duty to provide individuals with a privacy notice when their personal data is collected (see Processing personal data fairly and lawfully); and
- an individual's right to make a subject access request.

The non-disclosure provisions are:

- an organisation's duty to comply with the first data protection principle, but not including the duty to satisfy one or more of the conditions for processing (see Processing personal data fairly and lawfully) – you must still do this.
- an organisation's duty to comply with the second, third, fourth and fifth data protection principles;
- an individual's right to object to processing that is likely to cause or is causing damage or distress; and
- an individual's right in certain circumstances to have inaccurate personal information rectified, blocked, erased or destroyed .

An exemption from "the non-disclosure provisions" – which would, for example, allow you to disclose personal data that would otherwise be protected from disclosure – is not an automatic exemption from all (or any) of those provisions. This is because an exemption only applies to the extent that the provisions are inconsistent with the disclosure in question. So if you think you may be exempted from any of the non-disclosure provisions, you should consider each of those provisions in turn and decide:

- which, if any, would be inconsistent with the disclosure in question; and
- the extent of the inconsistency.

Disclosure and non-disclosure – when do the exemptions apply?

Several specific exemptions are set out in Part 4 of, and Schedule 7 to, the Data Protection Act. There are other exemptions in regulations made under the Act. The following are some of the exemptions that often apply.

Crime and taxation

The Act recognises that it is sometimes appropriate to disclose personal data for certain purposes to do with criminal justice or the taxation system. In these cases, individuals' rights may occasionally need to be restricted.

In particular, the Act deals with several situations in which personal data is processed for the following "crime and taxation purposes":

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

Personal data processed for any of these purposes is exempt from:

- an organisation's duty to comply with the first data protection principle, but not including the duty to satisfy one or more of the conditions for processing – you must still do this; and
- an individual's right to make a subject access request.

Example

The police process an individual's personal data because they suspect him of involvement in a serious crime. If telling the individual they are processing his personal data for this purpose would be likely to prejudice the investigation (perhaps because he might abscond or destroy evidence) then the police do not need to do so.

However, the exemption applies, in any particular case, only to the extent that applying those provisions would be likely to prejudice the crime and taxation purposes. You need to judge whether or not this effect is likely in each case – you should not use the exemption to justify withholding subject access to whole categories of personal data if for some individuals the crime and taxation purposes are unlikely to be prejudiced.

Example

A taxpayer makes a subject access request to HMRC for personal data they hold about him in relation to an ongoing investigation into possible tax evasion. If disclosing the information which HMRC have collected about the taxpayer would be likely to prejudice their investigation (because it would make it difficult for them to collect evidence, for example), HMRC could refuse to grant subject access to the extent that doing so would be likely to prejudice their investigation.

If, however, the taxpayer does not make the subject access request until some years later when the investigation (and any subsequent prosecution) has been completed, it is unlikely that complying with the request would prejudice the crime and taxation purposes – in which case HMRC would need to comply with it.

Nor would the exemption justify withholding all the personal data about an individual when only part of the personal data would be likely to prejudice those purposes.

Example

In the above example about an ongoing investigation into possible tax evasion, HMRC would be entitled to refuse subject access to personal data which would be likely to prejudice their investigation. However, this would not justify a refusal to grant access to other personal data they hold about the taxpayer.

Personal data is also exempt from the non-disclosure provisions if:

- the disclosure is for any of the crime and taxation purposes; and
- applying those provisions in relation to the disclosure would be likely to prejudice any of the crime and taxation purposes.

The Act does not explain "likely to prejudice". However, our view is that for these exemptions to apply, there would have to be a substantial chance (rather than a mere risk) that complying with the provision would noticeably damage one or more of the crime and taxation purposes.

Example

The police ask an employer for the home address of one of its employees as they wish to find him urgently in connection with a criminal investigation. The employee is absent from work at the time. The employer had collected the employee's personal data for its HR purposes, and disclosing it for another purpose would ordinarily breach the first and second data protection principles. However, applying those principles in this case would be likely to prejudice the criminal investigation. The employer may therefore disclose its employee's home address without breaching the Act.

If challenged, you must be prepared to defend your decision to apply an exemption, to the ICO or the court. So we advise you to ensure that any such decisions are taken at an appropriately senior level in your organisation and that you document the reasons for the decision.

These exemptions do not require you to disclose personal data to the police or to other law enforcement agencies – they merely keep you within the Data Protection Act if you decide to disclose information in the circumstances in which the exemptions apply. We have published guidance about Using the crime and taxation exemptions (pdf) and Releasing information to a private investigator (pdf) that give more advice on this.

Another limb of the crime and taxation exemption is that personal data which:

- is processed for the purpose of discharging statutory functions; and
- consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes

is exempt from the subject information provisions to the extent that applying those provisions to the personal data would be likely to prejudice any of the crime and taxation purposes. This prevents the subject information provisions applying to personal data which is passed to statutory review bodies by law enforcement agencies, and ensures that the exemption is not lost when the information is disclosed during a review.

Example

The Independent Police Complaints Commission (IPCC) begins an investigation into the conduct of a particular police force. Documents passed to the IPCC for the purposes of the investigation contain personal data about Mr A which the police force would not have been obliged to disclose to Mr A in response to a subject access request – because doing so would be likely to prejudice its criminal investigation. If Mr A then makes a subject access request to the IPCC, he has no greater right of access to the personal data in question.

There is another exemption that is designed to prevent the Data Protection Act being used to force public authorities to disclose information about the operation of crime detection and anti-fraud systems, where such disclosure might undermine the operation of those systems.

Regulatory activity

The Act provides an exemption from the subject information provisions for processing personal data in connection with regulatory activities. The exemption is not available to all organisations, and it applies only to the core functions of bodies that perform public regulatory functions concerned with:

- protecting members of the public from dishonesty, malpractice, incompetence or seriously improper conduct, or in connection with health and safety;
- protecting charities; or
- fair competition in business.

For the exemption to apply, those functions must also be:

- conferred by or under an enactment;
- functions of the Crown, a Minister or government department; or
- any other public function exercised in the public interest.

So the exemption applies to public functions exercised by various watchdogs whose regulatory role is recognised by the public and the sector they oversee. Such regulators may be established by law or as a result of mutual agreement between the participants in their sector of business. However, the exemption does not apply to investigatory or complaint-handling functions that may benefit the public but which organisations undertake when investigating their own activities. Functions like complaint handling, which are subsidiary activities of most organisations, do not fall within the scope of the exemption.

There is no blanket exemption for regulatory activities – not even for the activities that fall within the scope of the exemption. This is because personal data that is processed to perform such activities is exempt from the subject information provisions only to the extent that applying those provisions would be likely to prejudice the proper performance of the activities.

We have produced detailed guidance on the application of the regulatory activity exemption:

Regulatory activity (section 31)
For organisations
PDF (278.82K)

Publicly available information

Where an organisation is obliged by or under an enactment to make information available to the public, personal data that is included in that information is exempt from:

- the subject information provisions;
- the non-disclosure provisions;
- the organisation's duty to comply with the fourth data protection principle (accuracy); and
- an individual's right in certain circumstances to have inaccurate personal information rectified, blocked, erased or destroyed.

The provisions mentioned in the third and fourth bullet points form part of the non-disclosure provisions. However, they are mentioned separately here because there is an automatic exemption in these circumstances. There is no need for the organisation to show that the provisions are inconsistent with the disclosure.

Example

The Registrar of Companies is legally obliged to maintain a public register of certain information about companies, including the names and (subject to certain restrictions) addresses of company directors. A director complains that his name has been inaccurately recorded on the register. The Registrar is exempt from the director's right under the Data Protection Act to have the inaccuracy corrected (the Registrar's duties in relation to the register are governed by other legislation).

The exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about the individuals, the additional data is not exempt even if the organisation publishes that data.

Disclosures required by law

Personal data is exempt from the non-disclosure provisions if you are required to disclose it:

- by or under any UK enactment;
- by any rule of common law; or
- by an order of a court or tribunal in any jurisdiction.

In these circumstances, the legal obligation overrides any objection the individuals may have.

Example

An employer is legally required to disclose details of its employees' pay to HMRC in the usual course

of administering its PAYE arrangements. The employer may disclose this information irrespective of any objection which an employee may raise.

If you know that you are likely to be legally required to disclose certain kinds of personal data, it is good practice to tell individuals about this when you collect the information from them. This is because telling individuals about the legal requirement is compatible with the disclosure of personal data to comply with the requirement.

Legal advice and proceedings

Personal data is exempt from the non-disclosure provisions where the disclosure of the data is necessary:

- for or in connection with any legal proceedings (including prospective legal proceedings);
- for obtaining legal advice; or
- for establishing, exercising or defending legal rights.

You do not have to disclose personal data in response to a request from a third party simply because this exemption applies. You can choose whether or not to apply the exemption to make a disclosure, and you should do so only if you are satisfied that the disclosure falls within the scope of the exemption. In other words:

- it is necessary for one of the above purposes; and
- applying the non-disclosure provision would be inconsistent with the disclosure.

When faced with a request for disclosure, it can be difficult to decide whether the necessity test can be satisfied. You may also be reluctant to make a disclosure of personal data because of your relationship with the individual. In such circumstances you may decide not to comply with the request, unless obliged to do so under a court order.

Personal data is also exempt from the subject information provisions if it consists of information for which legal professional privilege (or its equivalent in Scotland) could be claimed in legal proceedings.

Confidential references

Personal data is exempt from an individual's right of subject access if it comprises a confidential reference that an organisation gives (or is to give) in connection with education, training or employment, appointing office holders, or providing services. The exemption only applies to references you give, and not to references you receive.

Example

Company A provides an employment reference for one of its employees to company B. If the employee makes a subject access request to company A, the reference will be exempt from

disclosure. If the employee makes the request to company B, the reference is not automatically exempt from disclosure and the usual subject access rules apply.

Management information

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the subject information provisions to the extent that applying those provisions would be likely to prejudice the business or other activity of the organisation.

Example

The senior management of an organisation is planning a re-organisation. This is likely to involve making certain employees redundant, and this possibility is included in management plans. Before the plans are revealed to the workforce, an employee makes a subject access request. In responding to that request, the organisation does not have to reveal its plans to make him redundant if doing so would be likely to prejudice the conduct of the business (perhaps by causing staff unrest in advance of an announcement of the management's plans).

Negotiations

Personal data that consists of a record of your intentions in negotiations with an individual is exempt from the subject information provisions to the extent that applying those provisions would be likely to prejudice the negotiations.

Example

An individual makes a claim to his insurance company. The claim is for compensation for personal injuries which he sustained in an accident. The insurance company disputes the seriousness of the injuries and the amount of compensation it should pay. An internal paper sets out the company's position on these matters and indicates the maximum sum it would be willing to pay to avoid the claim going to court. If the individual makes a subject access request to the insurance company, it would not have to send him the internal paper – because doing so would be likely to prejudice the negotiations to settle the claim.

Journalism, literature and art

This exemption protects freedom of expression in journalism, art and literature (which are known as the 'special purposes').

The scope of the exemption is very broad and it can exempt from most provisions of the DPA, including subject access – but never principle 7 or the section 55 offence (unlawful obtaining etc of personal

data).

However it does not give an automatic blanket exemption. In order for the exemption to apply:

- the data must be processed only for journalism, art or literature,
- it must be being processed with a view to publication,
- you must have a reasonable belief that the publication is in the public interest, and
- you must have a reasonable belief that compliance with the DPA is incompatible with journalism, art or literature.

You will need to explain why the exemption is required in each case, and how and by whom this was considered at the time. The ICO does not have to agree with your view – we must be satisfied that you had a reasonable belief.

We have produced detailed guidance on this exemption in our guide for the media. Whilst the focus of the guidance is journalism it will also be useful when considering applying the exemption to processing for artistic or literary purposes.

> Guide for the media
> For organisations

Domestic purposes

The most comprehensive exemption applies when personal data is processed by a data controller who is an individual (not an organisation) only for the purposes of their personal, family or household affairs.

Example

An individual keeps a database of their friends' and relatives' names, addresses and dates of birth on their PC. They use the database for keeping track of birthdays and to produce address labels for Christmas cards. The domestic purposes exemption applies to this type of processing.

Example

An individual records the highlights of their summer holiday on a digital camcorder. The recording includes images of people they meet on holiday. Although those digital images are personal data, the domestic purposes exemption applies.

None of the data protection principles apply in these circumstances, nor do any of the rights which the Act gives to data subjects. There is also no need to notify the ICO about processing for these purposes.

So there is an almost total exemption from the Data Protection Act for individuals who just use personal data for their own domestic and recreational purposes. However, the Act still applies to the extent that the ICO may investigate if someone seems to have gone beyond the scope of the exemption, and we may take enforcement action where necessary.

Read further guidance about when this exemption may apply to information posted on social networking sites or other online forums:

> Social networking and online forums – when does the DPA apply?
> For organisations
> PDF (292.7K)

Are there any further exemptions?

Yes. Exemptions are also available in relation to:

- national security and the armed forces;
- personal data that is processed only for research, statistical or historical purposes;
- personal data relating to an individual's physical or mental health. This applies only in certain circumstances and only if granting subject access would be likely to cause serious harm to the physical or mental health of the individual or someone else;
- personal data that consists of educational records or relates to social work;
- personal data relating to human fertilisation and embryology, adoption records and reports, statements of a child's special educational needs and parental order records and reports;
- personal data processed for, or in connection with, a corporate finance service involving price-sensitive information;
- examination marks and personal data contained in examination scripts; and
- personal data processed for the purposes of making judicial, Crown, or Ministerial appointments or for conferring honours.

Complaints

What happens when someone complains?

If a member of the public is concerned about your information rights practices, we believe that you, as the organisation responsible, should deal with it.

We expect you to respond to any information rights concerns you receive, clarifying how you have processed the individual’s personal information in that case and explaining how you will put right anything that's gone wrong.

If a member of the public has engaged with you but is still dissatisfied, they may report their concern to the ICO.

For further information, read:

How we deal with complaints and concerns - a guide for data controllers
For organisations
PDF (129.7K)

Anonymisation

What is anonymisation?

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. The Data Protection Act controls how organisations use 'personal data' – that is, information which allows individuals to be identified.

Organisations are increasingly reliant on anonymisation techniques to enable wider use of personal data. The code of practice explains the issues surrounding the anonymisation of personal data, and the disclosure of data once it has been anonymised. The code describes the steps an organisation can take to ensure that anonymisation is conducted effectively, while retaining useful data.



Anonymisation code of practice

This code will be useful to any organisation which wants to turn personal data into anonymised information for research or other data analysis purposes.

We've also produced a summary of the code (pdf) and a summary of the points raised during the consultation on the draft code (pdf).

Here's the ICO's Iain Bourne talking about the code. (NB: playing YouTube videos sets a cookie



And over on our blog the ICO's Head of Policy Steve Wood talks about anonymisation - opportunities and risks.

Anonymisation network

The ICO is supporting the establishment of a network for practitioners to discuss issues relating to anonymisation, and share best practice. The UK Anonymisation Network (UKAN) is co-ordinated by the University of Manchester, the University of Southampton, the Open Data Institute, and the Office for National Statistics.

UK Anonymisation Network (UKAN) website

Big data

Big data is a major topic of discussion across a number of fields, including management and marketing, scientific research, national security, government transparency and open data. Both public and private sectors are making increasing use of big data analytics. The ICO is interested specifically in the data protection and privacy risks posed by big data.



Big data and data protection

This paper provides an overview of the issues concerning big data, as we see them.





Summary of feedback on Big data and data protection and ICO response

This paper summarises the comments we received on our big data paper and gives our response to them.

This is an area in which the capabilities of the technology and the range of potential applications are evolving rapidly and there is ongoing discussion of the implications of big data. Our aim is to ensure that the different privacy risks of big data are considered along with the benefits of big data.

It is our belief that the emerging benefits of big data will be sustained by upholding key data protection principles and safeguards.

CCTV

The UK is recognised as a leading user of CCTV and the public are used to seeing CCTV cameras on virtually every high street. Such systems continue to enjoy general public support but they do involve intrusion into the lives of ordinary people as they go about their day to day business and can raise wider privacy concerns.

We know from our research that the public expect CCTV to be used responsibly with proper safeguards in place. We have therefore issued guidance to help organisations who use CCTV to comply with the Data Protection Act 1998 and to help them inspire public confidence that they are using CCTV responsibly.

Images of people are covered by the Data Protection Act, and so is information about people which is derived from images – for example, vehicle registration numbers. Most uses of CCTV by organisations or businesses will be covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.



CCTV code of practice

We have published this code of practice to help organisations using CCTV to stay within the law.

The CCTV code of practice provides guidance and advice for CCTV users on how to comply with the Data Protection Act and also includes a simple checklist for users of very limited CCTV systems where

the full provisions of the code would be too detailed.

CCTV in pubs

The ICO has received a number of enquiries from pub landlords on the issue of CCTV installation being made a condition for obtaining, or continuing, a licence to sell alcohol.

Further reading

ICO view of CCTV in pubs in England
For organisations
PDF (33K)

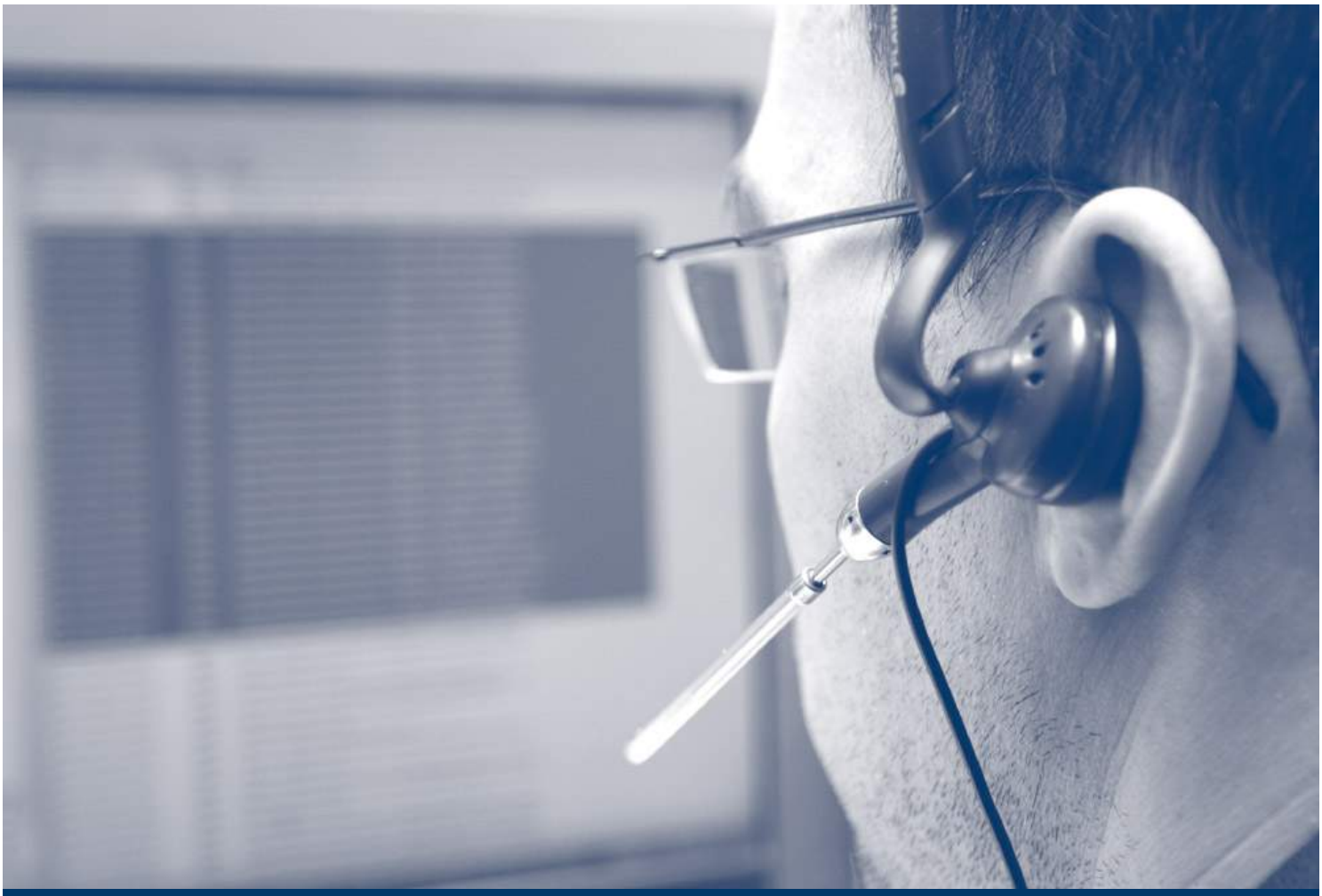
CCTV in pubs in England - FAQs
For organisations
PDF (45.24K)

Data sharing

The data sharing code of practice is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. The code explains how the Data Protection Act applies to the sharing of personal data.

It provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one off requests to share personal data.

Adopting the good practice recommendations in the code will help organisations to collect and share personal data in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.



Data sharing code of practice

This code of practice provides practical advice to any organisation that shares personal data.

Data sharing checklists

These two checklists provide a handy step by step guide through the process of deciding whether to share personal data. One checklist is for systematic data sharing, the other is for one off requests to share personal data.

Further reading

Data sharing checklists
For organisations
PDF (131.49K)

Data sharing checklists Welsh
For organisations
PDF (929.14K)

Employment

As an employer, you have responsibilities to ensure your employees' personal details are respected and properly protected.

Employment: quick guide

Our quick guide to the employment practices code (pdf) is ideal for small businesses and provides all the information you'll need to keep on the right side of the law. It covers:

- What the Data Protection Act means to an employer
- Recruitment and selection
- Employment records
- Monitoring at work
- Information about workers' health
- What rights do workers have?

Employment practices code

These guides cover the code in detail and provide answers to all the main questions you're likely to ask:

Employment practices code of practice
For organisations
PDF (694.77K)

Employment practices code supplementary guidance
For organisations
PDF (1.81MB)

Specific guidance

Disclosure of employee information under TUPE
For organisations
PDF (229.52K)

Subject access code of practice
For organisations
PDF (852.92K)

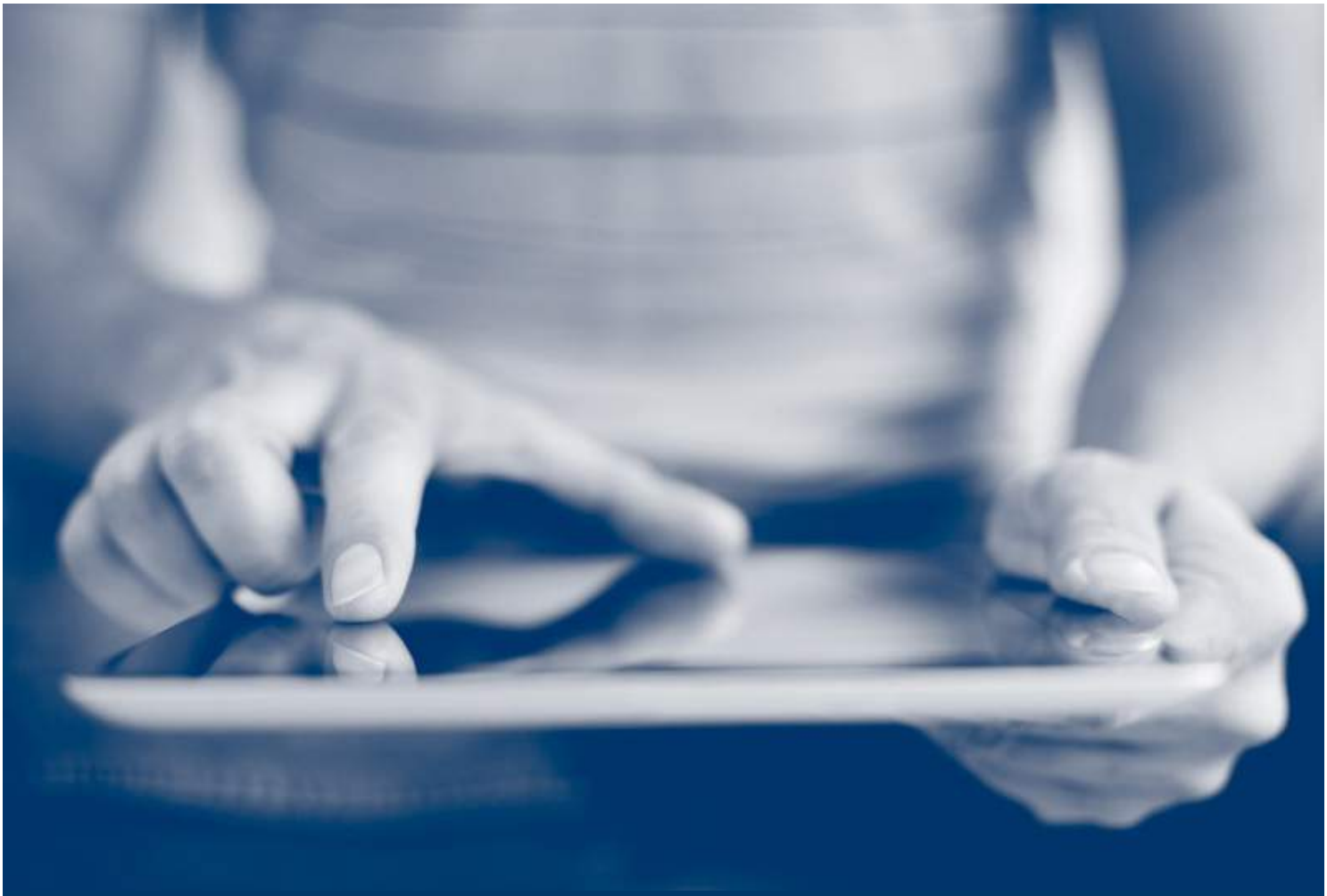
Monitoring under section 75 of the Northern Ireland Act 1998
For organisations

> PDF (150.59K)

Online and apps

Personal information online

More and more people are conducting their personal affairs online. Online shopping, social networking, job hunting and the ability to carry out 'official' functions, such as renewing car tax or contacting local councils and government departments online, are now an everyday part of life.



Personal information online code of practice

The code explains how the Data Protection Act applies to the collection and use of personal data online. It provides good practice advice for organisations that do business or provide services online. It was launched in July 2010 following an extensive consultation process.

The code explains the privacy risks that may arise when operating online, and suggests ways for organisations to deal with them. It stresses the importance of treating consumers' information properly, and being transparent about how their information is used.

The code covers topics including online marketing, operating internationally, and applying individuals' rights in an online environment. It applies equally to the public and private sectors.

On 26 May 2011 the rules on using cookies changed. This guidance reflects the law before that date.

Our advice on the new cookies law sets out the changes and explains what steps you need to take now to ensure you comply.

If you run a small business with an online presence, this checklist will help you to adopt best practice when processing your customers' information.

Personal information online: small business checklist
For organisations
PDF (447.41K)

Protecting personal data in online services

This report identifies eight of the most common IT security vulnerabilities that have resulted in organisations failing to keep people's information secure.

The flaws were identified during the ICO's investigations into data breaches caused by poor IT security practices. Many of these incidents have led to serious security breaches resulting in the ICO issuing monetary penalties totalling almost a million pounds.

Protecting personal data in online services: learning from the mistakes of others
For organisations
PDF (469.54K)

Your questions answered – video

Simon Rice, Group Manager for our Technology team, answers questions sent to us via Twitter and our WordPress blog about the report.



Mobile apps

As with any other business or project, developers of applications for mobile devices need to comply with the Data Protection Act.

A typical mobile ecosystem contains many different components, including mobile devices themselves, their operating systems, plus apps provided through an app store. In many ways these are simply developments of earlier concepts that have been used on less portable computer hardware for years, but the mobile environment has some particular features that make privacy a pressing concern.

In light of these features, this guidance has been produced to help app developers comply with the Data Protection Act 1998 and ensure users' privacy.

Privacy in mobile apps
For organisations
PDF (794.16K)

Wi-Fi analytics

Monitoring individuals through the use of Wi-Fi analytics can be a privacy intrusive activity unless specific actions are taken. This guidance has been developed to explain these risks and give advice to organisations considering the use of the technology.

Wi-Fi location analytics
For organisations

PDF (277.28K)

Privacy by design

What is ‘privacy by design’?

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

Although this approach is not a requirement of the Data Protection Act, it will help organisations comply with their obligations under the legislation.

The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

We would like to see more organisations integrating core privacy considerations into existing project management and risk management methodologies and policies.

Benefits of taking a ‘privacy by design’ approach

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are an integral part of taking a privacy by design approach. Our code of practice explains the principles which form the basis for a PIA.

Privacy impact assessments (PIAs) are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

You can integrate the core principles of the PIA process with your existing project and risk management

policies. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout your organisation.



Conducting privacy impact assessments code of practice

This guide explains what PIAs are and how you can use them in your organisation.

The code contains annexes which can be used as the basis for your PIA. These include questions to guide the process and templates for recording the assessment. You do not have to use these if you would prefer to follow your own process, but the annexes are included here in an editable format.

As part of our work in this area, we commissioned a report into the use of PIAs and the potential for further integration with project and risk management. The report was drafted by Trilateral Research and Consulting. You can access the report and an executive summary here.

ICO guidance and other resources

The ICO has a range of guidance and practical advice which can assist organisations when developing new projects.

- Anonymisation code of practice (pdf)
- Privacy notices code of practice (pdf)
- Data sharing code of practice (pdf)

Data science and PIAs

The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The framework can be a useful tool if you are working on a project involving data science, Big Data or analytics. If you are doing a PIA, the Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

Seven foundational principles of privacy by design

The Information & Privacy Commissioner of Ontario has taken a leading role in developing the privacy by design concept, establishing seven 'foundational principles of privacy by design'. These principles will be relevant for UK data controllers too.

> 7 Foundational Principles (Privacy by Design website)
> External link