Introduction to the Data Protection Act 1998 (DPA)
FAQ Fact Sheet

The DPA provides the structure that governs how your organisation should process any personal data that it holds. This FAQ overview document looks at common questions that you may have about the DPA and dealing with personal data. This fact sheet is part of a series of FA fact sheets on the operation and implementation of the DPA.

What is "personal data"?

Broadly speaking, data will be "personal" if it identifies a living individual. Anonymised data can also be "personal" under the DPA if, when put together with other data held by the organisation, a living individual can be identified from it. For example, if a spreadsheet is anonymised by using codes (such as "Person A") and the organisation holds a further spreadsheet decrypting those codes (e.g. "Person A = Joe Bloggs"), then both spreadsheets (when available together) will constitute personal data.

Are there any other types of personal data under the DPA?

Yes. There is a category of data called "sensitive personal data". This is personal data that is given a higher level of protection due to its sensitive nature, and relates to an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a trade union;
- physical or mental health or condition;
- sexual life;
- commission or alleged commission of any offence; or
- any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.

The DPA talks a lot about "processing" personal data. What does this mean?

"Processing" effectively encompasses anything that an organisation may do with personal data, and can cover a range of actions, including receiving, sending, accessing, amending or transferring/sharing data.

What is a "data controller"?

A data controller is the "owner" of the personal data and is responsible for ensuring that it is processed in accordance with the DPA. A data controller is not normally an individual but will be the organisation responsible for the data held. For example, for a club the data controller is the club itself, not the club secretary or any other individual.

Does the DPA only cover computer records?

No. The DPA covers all personal data in whatever format that data may be held, including:

- Videos/tapes;
- CCTV footage;
- Electronic records;
- Paper files;
- Emails;
- Meeting notes;
- Expressions of opinions; and
- Photographs.

What are our organisation's obligations under the DPA?

You should comply with the eight data protection principles. This means that any processing of personal data must be:

1. processed fairly and lawfully;
2. processed for specific purposes;
3. adequate, relevant and not excessive;
4. kept accurate and up to date;
5. not kept for longer than is necessary;
6. processed in accordance with the rights of individuals;
7. kept secure; and
8. not transferred outside of the EEA.

How do I know if I am processing personal data "fairly and lawfully"?

This requirement (set out in the 1st Data Protection Principle) goes to the heart of the DPA. It means that you should:

- have lawful and justifiable reasons for collecting/processing the personal data;
- be transparent about why you are collecting the data and how you are going to use it;
- not use personal data in a way that may cause damage or distress, or in a way that the individual would not expect; and
- not do anything illegal with the data (obviously!).

How can I be transparent about the data I am processing?

One way of making sure that individuals are informed is to provide them with a "privacy notice".

This does not have to be a formal document but should be easily accessible by individuals (i.e. available to them at the time that you collect the data). It should contain certain information such as who you are, why you are processing their data, and what you are going to do with it.

What if I get a complaint about the way in which we have handled someone's personal data?

Any such complaint should be treated seriously and action taken where appropriate. Individuals have the right to ask you to:

- correct (or delete) any information that you hold about them that is wrong;
- stop sending marketing materials; or
- (in some circumstances) stop processing their data altogether.

If in doubt, seek specialist advice.

Do I have any other obligations?

Yes. You must also respond to requests to see personal data that you may hold on an individual, where that individual requests it. These are known as Subject Access Requests. Please see our "Subject Access Requests" fact sheet for more details. You should also consider whether you are required to "notify" the ICO of the processing that you are carrying out. You can find an explanation of this process in our "Notifying the ICO" fact sheet.

Who is the ICO and what is its role?

The Information Commissioner's Office (ICO) is the body responsible for enforcing the DPA. It has a range of powers in the event that an organisation breaches the DPA, including:

- imposing fines of up to £500,000;
- requiring organisations to sign undertakings to improve processes and compliance; and
- undertaking compulsory audits.

The ICO is also a source of advice and operates a helpline for DPA related enquiries on **0303 123 1113**.

Data Protection and Marketing

FAQ Fact Sheet

This fact sheet looks at the circumstances in which personal data can be used for marketing.

What does the DPA have to do with marketing?

The DPA governs the use of personal data in marketing and is supplemented by the Privacy and Electronic Communications Regulations **(PECR)**, which apply to electronic marketing and the use of "cookies".

What does the PECR say?

The PECR says that you cannot send unsolicited electronic communications (including by text/email) to individuals unless they have consented to receiving those communications. This means that you cannot take information you have collected for one purpose (for example, membership lists) and use it to send electronic marketing information without consent.

How do I get consent?

You should ask the individual for permission to send electronic marketing information at the time that their details are collected, and record the consent (or refusal) accordingly.

Is there any way to send electronic marketing information without consent?

There is an exemption known as the "soft opt in". This is quite complex but means that you do not need consent where:

- you obtained the contact details during the sale of products or services to that individual; **and**
- the marketing information relates to the same or similar services; **and**
- the individual has been given an opportunity to refuse marketing information at the time that their contact details were collected, and at the time of each marketing communication.

This is a complex exception and it is recommended that consent is obtained.

What information do I have to provide when sending electronic marketing information?

You must ensure that your identity is not concealed and you must provide a valid address that the individuals can contact to opt out of future marketing.

Where can I find more information?

The ICO has produced a very detailed guide on the PECR which can be found at **www.ico.org.uk** If you are planning to use "cookies" on your website, please see the "Cookies" FAQ Fact sheet.

CCTV
FAQ Fact Sheet

This fact sheet looks specifically at CCTV and your organisation's obligations under the Data Protection 1998 (DPA) when using CCTV.

What does CCTV have to do with data protection?

CCTV images are classed as personal data where individuals can be identified from them. As a result they are subject to the same protections as other personal data.

What does this mean for us as an organisation?

This means that you will have to take into account the rights of individuals when operating a CCTV system, including the siting of cameras. Cameras should minimise the impact on an individual's privacy and should not be positioned on unnecessary areasor where employees/visitors would expect privacy (such as bathrooms).

What other obligations do we have?

You should ensure that clear signage is displayed to raise awareness that CCTV is used, who it is operated by and for what purpose. You should also ensure that controls are in place around access to the images.

What sort of controls?

CCTV control rooms should be sited in a secure areas and only specifically authorised individuals should have access to the images.

What if I get a request for access to the images?

You may get a request for CCTV images as a result of a subject access request (please see our separate "Subject Access" factsheet) and these requests should be treated in the same way as any other access requests for personal data. When providing images in response to a subject access request you should try to minimise any impact on the privacy of others; for example not providing the entire tape and instead providing the relevant parts affecting the individual.

What if the request is from the police?

Please see our separate "Data Protection and the Police" fact sheet.

For how long should I keep CCTV images?

These images should not be kept for longer than is necessary – please see the "Records Management" fact sheet for a more detailed explanation.

Is there anything else I can do to make sure my organisation complies with the DPA?

The ICO has produced the CCTV code of practice, which is a helpful guide for organisations using CCTV. It can be found at www.ico.org.uk

Children and Data Protection

FAQ Fact Sheet

This fact sheet looks at specific issues around children and the Data Protection Act 1998 (DPA) in the context of subject access requests. Please also see our "Subject Access Requests" fact sheet.

What do I do if I receive a subject access request for information about a child?

You should carefully consider any request for information about a child. Whether the request has originated from the child or a guardian, you should make a judgement as to whether the child is mature enough to understand its rights.

How will I know if a child is mature enough?

The child must be able to broadly understand what a subject access request is and to understand the information they will receive. When making this decision you should consider:

- the individual child's maturity;
- the personal data in question;
- the views of the child;
- any relevant court orders;
- any duty of confidence owed to the child; and
- any likely consequences of disclosure (this is particularly important if a parent or guardian has requested the data and the data involves allegations against that parent or guardian).

What if I decide that the child is mature enough but the request has come from a parent/guardian?

A parent/guardian does not have an automatic right to the personal data of the child. If the child has not consented to the disclosure, or if you are unsure, you should reply directly to the child rather than the parent/guardian.

Is there an age that a child is presumed to be mature?

In Scotland there is a presumption that a child of 12 or older is mature enough for the purposes of the DPA. This does not apply in England but gives an indication of what may be considered reasonable.

Anything else?

If you receive a request for information about a child (whether from a parent/guardian, or third party organisation such as the police or social services), please think carefully before complying. If in doubt, please seek specialist advice.

Cookies

FAQ Fact Sheet

This fact sheet looks at the rules around using cookies on your organisation's website.

What are cookies?

A "cookie" is a small text file that is placed onto a device (e.g. a computer or mobile device) when the user accesses some websites. They enable the website to "recognise" a user and are often used by website operators (for example by using Google Analytics) to improve the performance of their website.

What law applies to the use of cookies?

Similarly to electronic marketing, the Data Protection Act 1998 and the Privacy and Electronic Communication Regulations **(PECR)** both apply to the use of cookies where personal data is collected.

Can we use cookies on our website?

Yes, if you have the user's consent. Depending upon the type of cookies used on your site, you will require differing levels of consent.

What do you mean?

The ICO has confirmed that if an organisation uses nonintrusive, session cookies such as Google Analytics, the implied consent of the user may be enough.

What do you mean by "implied consent"?

You must tell visitors to your site about any cookies that you use, and this information must be prominently displayed. Many websites (including the ICO website) choose to display this as a banner at the top of the web page. If intrusive cookies are used, the user should be required to click "I Accept" on this banner before proceeding onto the website. This is explicit consent. However, if cookie usage is minimal, a user may be able to simply proceed through the website without clicking "I Accept". They are accepting the cookies impliedly by continuing to use the site. This is implied consent.

Sounds great!

Yes, if you have the user's consent. Depending upon the type of cookies used on your site, you will require differing levels of consent.

How do I find out more?

The ICO has confirmed that if an organisation uses nonintrusive, session cookies such as Google Analytics, the implied consent of the user may be enough.

Data Protection and the Police

FAQ Fact Sheet

This fact sheet looks at data protection in the context of police requests and in particular what you should do if the police request personal data held by your organisation.

PC Smith of Northumbria Police called me this afternoon and asked me for a player's address and contact details – what do I do?

Firstly, don't panic! The Police do not have an automatic right of access to personal data, and you are under no obligation to provide this information.

So if I provide this information will I breach the DPA?

Not necessarily. Providing this information voluntarily will not be a breach of the DPA provided that:

1. the personal data is needed for the purpose of preventing or detecting crime, or for apprehending/prosecuting offenders; and
2. not disclosing the personal data will prejudice these purposes.

But how do I know if this is the case?

You should ask the Police to confirm this. In order to obtain authentication, you should ask that the request is made in writing and signed by a senior police officer. The written request should specify the reason for the request and confirm that (in the police's opinion) failing to provide the information would prejudice their investigation. If it is possible to respond to the query without releasing personal data, you should do so.

What if I am still not sure whether data should be released?

As highlighted above, you are under no obligation to release the data. If you have good reason not to (if, for example, you are under a confidentiality obligation), you can refuse the request and ask that the police return with a court order. You will not be in breach of the DPA if you comply with a court order.

Data Security

FAQ Fact Sheet

Any organisation processing personal data is required to take appropriate organisational and technical measures to keep that data secure. The DPA does not specify exactly what is required, and this fact sheet looks at common issues in this area.

So what does "appropriate organisational and technical measures" mean in reality?

In a nutshell, it means your organisation must have sufficient security to prevent personal data being lost, damaged or inappropriately accessed. This is not just electronic measures such as firewalls, but physical measures such as building access, and organisational measures such as policies and procedures.

What level of security am I required to have in place?

The DPA says that you should have security that is appropriate and proportionate to:

- the nature of the information; and
- the harm that may result from improper use, loss or destruction of that information.

This means that you are not expected to install cutting edge expensive technology, but should assess the risks that may arise from the data that you hold and ensure that the security you have is appropriate for those risks. You should also continuously review your arrangements so that they are relevant and up to date.

Surely it's not that big a deal – what's the worst that could happen?

A breach of data security can be serious and can cause harm, inconvenience and distress to individuals. A breach can also have wider implications where personal data falls into the wrong hands and can lead to identify theft, fraud and also in some cases expose witnesses to intimidation.

What else should I do to make sure our measures are appropriate?

As well as carrying out a risk assessment, someone within your organisation should be identified as having day to day responsibility for security issues. It is important that this person has enough authority and access to resources to fulfil this role.

Depending on the size of your organisation and the amount of personal data that you process, you should consider putting in place an information security policy. This does not have to be overly formal or lengthy, but should cover:

- access to IT equipment, proper files and premises for staff and third parties (including any volunteers or temporary staff);
- business continuity/disaster recovery;
- key individuals should be identified, and any related processes For example, who is responsible for data security general, also is responsible for acting on any data breaches etc.

What about organisational measures?

This will include not only putting in place policies, but making sure that staff are trained and aware of their obligations under the DPA. Staff training should cover:

- basic obligations of the organisation and expectations of staff, including the consequences of breaching the DPA;
- proper procedures such as subject access, including identification requirements if staff are unsure, or if individuals try and access personal data over the telephone;
- any remote working procedures and restrictions on use of personal devices. You should also ensure that any staff accessing personal data are reliable and clear on what they can and cannot do with personal data.

What if we outsource some of our processing?

It is common for organisations to outsource some of its personal data processing, for example, some payroll functions or IT services. This scenario is considered in more detail in the "Outsourcing Services" fact sheet.

What happens if we lose some personal data?

It is crucial that you deal with any security breach quickly and effectively. You should have in place a protocol for dealing with breaches, regardless of whether they have arisen from accidental loss, theft or malicious act. This protocol should ensure that someone has overall responsibility for security breaches and should set out the following:

- containment and recovery plan, including limiting damage;
- risk assessment;
- notifying appropriate individuals that the breach has happened; and
- reviewing your organisation's response to the breach and making any necessary changes to your policies as a result.

Employment and Personnel Records
FAQ Fact Sheet

This fact sheet looks at the impact of the Data Protection Act 1998 (DPA) on the use, storage of and access to employee records.

How does the DPA impact on us in an employment context?

As well as your general obligations under the DPA, there are a number of issues that can arise in an employment context that impact on an individual's rights. These include:

- CCTV;
- monitoring of staff emails;
- employment references;

Please see our separate "CCTV" and "Records Management" fact sheets for further information about operating CCTV in the workplace and records management.

What are my general obligations in relation to employment records?

You should:

- ensure that employees know how you will hold information about them and whether you will disclose the information to anyone;
- ensure that those with access to employment records are aware of their obligations and how they should be handling data;
- regularly review data held about employees and cleanse any data that is no longer up to date, is no longer relevant, or is excessive;
- be careful not to make inappropriate disclosures of employee records.

We would like to monitor our staff members' emails, can we do this?

Any monitoring of employees is governed by the DPA. Whilst it does not generally prevent monitoring, the DPA says that where such monitoring has an adverse effect on workers, it must be justified by its benefit to the organisation (or other third parties).

What does this mean from a practical perspective?

You must be open with your employees about any monitoring. This means being clear about the scope of the monitoring that you intend to carry out.

How can I achieve this?

If you intend to carry out ongoing monitoring of employees, you should have a policy that clearly sets out the type of monitoring you will carry out and the reasons behind it. You must only use any data collected through such monitoring for the purposes for which it was collected.

What if we accidentally uncover something as a result of this monitoring?

If you uncover something that no reasonable employer would ignore (such as criminal activity or breach of health and safety rules that would put others at risk), you are entitled to act on this even if it is outside the scope or purpose of the original monitoring.

What other obligations do we have when monitoring employees?

You must keep all information gathered from monitoring secure and only those who absolutely need to access it should do so. You should also only keep the data for so long as is necessary.

What if I need to carry out monitoring without telling an employee?

This type of monitoring is extremely difficult to justify. This must also be authorised at the highest level possible in your organisation. As a minimum you must be satisfied that you have grounds for suspecting criminal activity and that informing the individual(s) in question would prejudice the outcome. It should be used sparingly in relation to a specific investigation only (rather than in response to general misgivings about an individual).

We gave a reference for one of our ex employees and they have asked us for a copy of it, do we have to provide it?

No. An individual must make a request to the organisation that has received the reference, rather than the one that sent it.

Is there any other information available about how we should be treating employee data?

Yes. The ICO website at www.ico.gov.uk has a great deal of information relating to this area. In particular, the "Employment Practices Code" and related "Quick Guide" will provide a more detailed overview.

Notifying the Information Commissioners' Office (ICO)
FAQ Fact Sheet

This fact sheet deals with an organisations' obligations to notify the ICO that it is processing personal data under the Data Protection Act 1998 (DPA)

What exactly is "notification"?

Notification is simply letting the ICO (and the public) know about the personal data that you process. The information about your organisation that you provide to the ICO is entered onto a register at www.ico.org.uk, which can be viewed by anyone with on-line access.

We don't process much personal data, surely this doesn't apply to us?

If your organisation processes any personal data it is likely that you notify. However, some organisations, such as charities are exempt from notification. Also, if you only process very basic personal data, your organisation may be exempt. If you are unsure you should take the simple quiz at www.ico.org.uk.

What if I need to notify but choose not to?

If you are required to notify and do not, this is a criminal offence. Even if you think that your organisation is exempt, you may choose to notify the ICO voluntarily.

How much will notification cost?

For most organisations it costs just £35 per year to notify. Organisations that have a turnover of £29.5m or more and have more than 249 members of staff will have to pay £500, as will public authorities with more than 249 members of staff.

How do I notify?

You can register online at **www.ico.org.uk**

Notifying the Information Commissioners' Office (ICO)
FAQ Fact Sheet

This fact sheet deals with an organisations' obligations to notify the ICO that it is processing personal data under the Data Protection Act 1998 (DPA)

Do I need to do anything else once I have notified the ICO?

Yes – you must make sure that your notification details are kept up to date, especially if there are major changes in the nature, range or way in which that you process personal data. You must also renew your notification each year. The ICO will usually send you a reminder letter before the renewal date.

I already have a notification, but I need to make some changes. How do I do this?

You can change your notification by emailing **registration@ico.org.uk** with your registration and security numbers. Changes will be made free of charge. If you need to make changes because your organisation has changed its legal status, you will need to submit a new registration.

How long does the notification process take?

This varies but you should usually receive a draft registration from the ICO within a week of making an online request.

Outsourcing Services

FAQ Fact Sheet

This fact sheet looks at the implications of the Data Protection Act 1998 (DPA) when using third parties to process personal data.

What types of services are relevant here?

Any service that your organisation (as a data controller), outsources to a third party and which involves the processing of personal data by that third party. This might include outsourcing of payroll functions, marketing or IT services.

What is a "data processor"?

The third party providing the outsourced services on your behalf is called a "data processor".

Who has responsibility for the data processor's compliance with the DPA?

You do. Data processors are not (currently) subject to the DPA directly. Whether you use a data processor or not, your organisation is liable for all personal data that it holds.

Are there any obligations on us when selecting a data processor?

Yes. The DPA contains specific provisions around selecting and engaging a data processor. You must:

- Select a processor that can provide guarantees around its data security; and
- take reasonable steps to make sure that the promised security processes are in place.

Any standards guaranteed by the processor must, as a minimum, meet the standards you would have met, had you processed the data yourself.

What else?

You must put in place a written contract that details what the processor may and may not do with the personal data. This does not have to be a separate written contract, and can be incorporated into the general contract for services between your organisation and the data processor. However, the European Committee for Standardisation has published a model processing contract that you may find useful. Details of this can be found at www.ico.org.uk.

Records Management

FAQ Fact Sheet

This fact sheet looks at what the Data Protection Act 1998 (DPA) says about retention and disposal of records

What does the DPA say about how long I should keep personal data for?

The DPA does not set out any specific maximum or minimum retention periods for personal data. The DPA says that personal data should "not be kept for longer than is necessary" for fulfilling the purpose for which it was collected.

What does that mean?

From a practical perspective, you should:

- review the data that you hold and the period for which you are holding it;
- in deciding how long to hold data, look at why you are holding it; and
- update (or delete) out of date data and data that is no longer needed.

What are the risks of retaining personal data indefinitely?

This will make it harder to comply with your obligations under the DPA to keep personal data up to date, and to not store excessive data. It will also make it difficult to respond to subject access requests.

Do I need a formal retention and disposal policy?

Not if you only process a small amount of personal data. If you process more than a small amount it is good practice to look at putting in place standard retention periods for certain categories of data (taking into account organisational needs and any sector-specific requirements).

How do I work out the length of the retention periods?

Organisational needs will be based on:

- a costs and risk assessment of retaining the information;
- the value of the information (both now and in the future);

and

- how easy it is to keep the information up to date.

For example, if an individual ceases to be a season ticket holder, the expectation is that this information would then be deleted, unless there is some other reason for keeping it (for example, if they were also an employee of the club).

If, as in the example above, you hold data about an individual in more than one capacity, you are not obliged to delete both sets of data in the event that one category becomes irrelevant or out of date (in this case, the information relating to the season ticket).

Are there any other legal requirements for retention periods?

There are a number of legal/professional requirements for keeping certain information for a specified period of time, for example to defend a claim, or for tax or health and safety reasons. Regardless of the timeframes, you must ensure that data is held securely at all times.

What happens at the end of the retention period?

The data should be reviewed and deleted/destroyed unless there is a good reason for keeping it.

What if we share the information with another organisation?

You will need to agree an appropriate retention period between you.

Social Media
FAQ Fact Sheet

This fact sheet looks at the implications of social media on your organisation and how it interacts with the Data Protection Act 1998 (DPA).

What does social media have to do with data protection?

Social media is widespread and is used by many as a method of personal communication in the same way as texts and email. It can be a useful tool but if used inappropriately, personal data can be compromised as a result of inappropriate disclosure.

What is the risk to the organisation?

Inappropriate or malicious use of corporate and personal social media accounts (for example someone using their Facebook page to openly discuss a grievance) can result in embarrassment for the organisation, aggrieved employees (if they are the target of malicious communications) and potential media interest.

What can I do to reduce this risk?

You should have clear policies in place which set out what is expected of employees when using social media for work or personal purposes. This policy should be rolled out to employees and enforced. If you require specific actions from individuals (for example to set their Facebook privacy settings to private) then you should ensure that they understand how to do this and support them.

What other practical steps can I take?

If your organisation uses social media for corporate purposes (for example, using LinkedIn or having an official Twitter feed), you should have in place clear controls and processes in the event that the employee leaves and make sure that passwords are changed as responsibilities do.

What about social media outside of the organisation – surely I can't control that?

Often damaging comments are made outside an organisation and sites (such as fan forums), can contain strong opinions on a range of subjects! If you have particular trouble with third parties that have a connection to the club or league (for example as a season ticket holder) then you could consider imposing a policy on them at the point that they apply for their tickets, setting out expected behaviours. You can then make it clear what the consequences of not following the policy would be (i.e. forfeiture of their ticket).

What about individuals who aren't connected to the club or league?

If you are having difficulty with a third party, that has no connection to the club or league and is posting content online, it is more difficult to address this. You should consider whether the comments may be defamatory (seeking specialist legal advice if necessary) but in many cases it will be difficult to identify the poster. In these cases you may need the cooperation of the internet service provider or the police before you are even in a position to take action. Always take legal advice if you think that any post might be breaking the law.

Subject Access Requests

FAQ Fact Sheet

This fact sheet looks at how you should deal with subject access requests (SARs) submitted under the Data Protection Act 1998 (DPA).

What is an SAR?

Section 7 of the DPA gives individuals the right to contact an organisation and request a copy of any personal data that is held by that organisation about them. This is called "the right of subject access". A request made under section 7 is called a subject access request or 'SAR'.

What information is a requestor entitled to?

An individual is entitled to:

- be told whether their personal data is being processed;
- be given a description of that data, including the reasons for which it is being held, the source of the data, and whether it has been/will be given to any third parties; and
- be given a copy of their personal data.

Can a requestor ask for personal data about other people?

No. Individuals are only entitled to their own personal data, unless they are validly acting on behalf of another individual when making a request.

Someone has made a request over the telephone. Is it valid?

No. In order to be valid a request must be in writing. You do not need to respond to verbal requests but it is good practice to at least explain that the request should be made in writing, rather than ignoring the individual altogether.

I am not sure the requestor is who they say they are. Do I still have to respond?

No. Under the DPA you are entitled to ask for two things before responding to a SAR:

1. ID information. This is to avoid accidental disclosure of personal data to the wrong person. This will not always be necessary, but should be requested if you have any doubt as to the identity of the requestor; and
2. any information reasonably necessary to find the personal data that is being requested, if it is not immediately apparent/ This could include keywords abbreviations or locations.

In both cases the clock for responding to a SAR will not start ticking until you have this information.

How long do I have to respond to an SAR?

You must respond to an SAR promptly, and in any event, within 40 (calendar, not working) days of receiving it, so long as you have the information set out above.

Do I have to provide all of the information that has been requested?

Not necessarily. There are a number of exemptions that relate to certain types of information, including information relating to:

- crime and taxation;
- legal advice and proceedings;
- management information; and
- negotiations with the requestor.

The main purpose of these exemptions is to ensure that data is not released that could prejudice the organisation or third parties (such as an ongoing police investigation or redundancy process).

Can I charge for responding to an SAR?

Yes. You are entitled to a maximum fee of £10 but you are not obliged to do so. If you do charge, you do not have to respond to the request until you have received the fee.

I have received a request for some information but I would like to amend it before sending it out. Can I do this?

This will depend upon the nature of the information. If the request is for information that is routinely updated, then a SAR should not prevent you from updating the information. However, if the information is not routinely updated, and you want to amend it for other reasons, this is not allowed.

Can someone submit a SAR on behalf of someone else?

Yes, this is quite common in certain circumstances, such as a solicitor asking on behalf of a client, or where an individual does not feel comfortable asking themselves. You must be satisfied that the requestor is authorised to act on behalf of the individual concerned, and you are entitled to ask for proof of this. If the individual is a child, please see our fact sheet on "Children and Data Protection".

What if the requestor asks for information that includes data about other people?

Information involving other people (known as 'third party data') is a difficult area and often crops up in grievances (for example in situations where witness statements are given). Generally, you do not have to comply with the request if it will involve discussing third party data, unless the third party has given their consent, or it is reasonable for you to disclose such third party data without their consent.

How will I know if it is reasonable to disclose without consent?

You should consider a number of factors, including:

- do you owe a duty of confidentiality to that third party?
- the specific facts of the case – is disclosure likely to result in any harm to the third party?
- Have you tried to get consent, and if so, has consent been refused?

I keep receiving the same (or very similar) requests from the same individual repeatedly. Do I have to keep sending out the same information?

There is no limit on the number of SARs that an individual can submit. However, you are not required to comply with repeated, identical requests unless a "reasonable interval" has elapsed. The DPA does not specify what a reasonable interval will be, but you should consider:

1. the nature of the data – is it often updated, or is it particularly sensitive?
2. why is the data being held? Is the processing likely to cause a detriment to the individual?

If the data is 'live' and is often amended/updated, or is of a particularly sensitive nature, you should consider complying with the request.

Transferring Personal Data outside the EEA
FAQ Fact Sheet

This fact sheet looks at when personal data may be transferred outside of the EEA, and the restrictions around such transfers.

What does the DPA say about transferring data outside the EEA?

The DPA says that personal data must not be transferred outside of the EEA unless the country receiving the personal data has in place an "adequate level of protection" for the rights and freedoms of individuals.

When might this apply?

This will be relevant not only for organisations with offices or business partners outside of Europe, but also for organisations that outsource activities (including call centres) to these areas. It will also apply if you use providers of certain services (such as IT cloud hosting) and the provider's servers are located outside the EEA.

What exactly counts as "the EEA"?

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

Austria	Belgium	Bulgaria	Cyprus
Czech Republic	Denmark	Estonia	Finland
France	Germany	Great Britain	Greece
Hungary	Ireland	Italy	Latvia
Lichtenstein	Lithuania	Luxemburg	Malta
Netherlands	Norway	Poland	Portugal
Romania	Slovakia	Slovenia	Spain
Sweden	Switzerland		

Are there any other countries that have an "adequate level of protection"?

Yes. The European Commission may decide from time to time (having assessed the protections in place), that certain countries have an adequate level of protection. Currently those countries are:

- Andorra;
- Argentina;
- Canada;
- Faroe Islands;
- Guernsey;
- Isle of Man;
- Israel;
- Jersey;
- Switzerland;
- Uruguay.

These are updated from time to time. The updated list is available on the Europa website at **www.ec.europa.eu.**

What if the country to which I want to transfer data doesn't sit on either of these lists?

If you are satisfied that the country has an adequate level of protection, you may still be able to proceed. You could:

- assess adequacy yourself (this is a complex procedure involving a risk assessment and completing paperwork to document this assessment);
- use model contracts approved by the European Commission;
- apply for approval for a binding set of guidelines known as "binding corporate rules – this is particularly useful for intraorganisational transfers involving overseas offices; or
- rely on other exemptions, such as consent. However, this should be a last resort.

If the receiving country is the USA, you could check to see if the organisation is registered with the "Safe Harbor" Scheme. You can do this at **http://safeharbor.export.gov/list.aspx**