

Personal information online code of practice



Introduction	5
1. About this code	6
2. How does the Data Protection Act apply to information processed online?	9
3. Marketing your goods and services online	19
4. Privacy choices	25
5. Operating internationally	28
6. Individuals' rights online	32
7. Things to avoid	36
Annex: Preserving privacy online	38
Glossary	40

Introduction

To help you navigate this book better look out for these markers



Link to a web page



Good practice tip –
Advice on what's good to do



Bad practice –
Advice on what NOT to do

The online world is expanding and developing all the time. Change is a given. And the pace of change is a challenge. New technologies and services are transforming the way we do business. The accelerating take-up of social networking, email, e-commerce and e-government reflects our growing dependence on the internet to conduct business, whether personal or professional.

The internet can offer greater convenience and new experiences, but it can also present risks. A record of our online activity can reveal our most personal interests. This is as true of major electronic service providers as it is of small online businesses. This code explains the privacy risks that may arise and suggests ways for organisations to deal with them. It stresses the importance of transparency, of treating consumers' information properly and being straight with people about how you use their information. This applies just as much in the public sector as it does in the private.

As regulator of the Data Protection Act I recognise the need for clear, comprehensive guidance for handling personal data properly and for giving individuals the right degree of choice and control. I encourage the industry to continue to develop simpler, easier ways for individuals to manage their online choices and to protect their privacy.

This is a fast-moving field of activity where the law may sometimes be difficult to interpret. I hope this code will help all organisations comply with the law, adopt good practice and prosper online.

Christopher Graham
Information Commissioner

1

About this code

This code explains how the Data Protection Act 1998 (the DPA) applies to the collection and use of personal data online. It also provides good practice advice for organisations that do business online and are therefore subject to the DPA.

The code covers the collection and use of personal data online, whether it is collected via a PC, games console, mobile device, media player or any other equipment that connects to the internet. It covers obvious identifiers, such as names, email addresses or account numbers obtained, for example, through an electronic application form. It also covers less obvious identifiers, such as information indicating individuals' online activity generated through the use of cookies and other identifiable monitoring, such as the analysis of IP addresses.

The code covers activities such as:

- collecting a person's details through an online application form;
- using cookies or IP addresses to target content at a particular individual;
- using personal data to market goods or to deliver public services; and
- using cloud computing facilities to process personal data.

This code does not cover the use of information that does not, or could not, identify an individual - for example the collection of anonymised or statistical information. The DPA does not apply to such activity. Nor does it apply to activities such as displaying the same broadcast-type content to everyone who visits a website - for example showing the same adverts for flights to everyone who visits a travel site.

Cookies

Many websites use cookies to remember information about which content has been accessed by a device. They can use this to keep people signed-in to a website between sessions, or to apply accessibility preferences to the pages. Many users and publishers find these uses of cookies to be convenient. The publisher needs to make users aware of the use of cookies, and should not do anything unexpected or intrusive with the information they collect.

Third party behavioural advertising

These adverts have been placed by an advertising network to which the publisher is affiliated. The publisher has chosen the adverts based on which other affiliated websites have been visited by the user. This information is linked by an identifying cookie on the user's machine, which can be accessed by the network but not the publisher.

First party behavioural advertising

These adverts have been placed on the page by the publisher. They contain recommendations for purchases based on the previous behaviour of the user. Because the adverts are targeted at users and use analysis of their past purchases, the publisher may be processing personal data about the user.

Untargeted advertising

Untargeted adverts can be placed by the publisher or an advertising network. The adverts could be randomly selected, and aren't based on website content or user behaviour. These adverts are unlikely to involve the processing of personal data by the publisher or network.

How the code can help

Adopting the good practice recommendations in this code will help you to collect and handle personal data in a way that's fair, transparent and in line with the wishes and expectations of the people you collect information about.

Specific benefits include:

- greater trust and a better relationship with the people you collect information about;
- reduced reputational risk caused by the inappropriate or insecure processing of personal data;
- better take-up of online services, meaning economic savings and greater convenience for customers;
- minimised risk of breaches and consequent enforcement action by the Information Commissioner or other regulators;
- gaining a competitive advantage by reassuring the people you deal with that you take their privacy seriously;
- increasing people's confidence to provide more valuable information, because they are reassured that it will be used properly and kept securely; and
- reduced risk of questions, complaints and disputes about your use of personal data.

The code's status

The Information Commissioner has issued this code under section 51 of the DPA in pursuance of his duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act.

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

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

We have tried to distinguish our good practice recommendations from the legal requirements of the DPA. However, there is inevitably an overlap because although the DPA sets out the bare legal requirements, it provides no guidance on the practical measures that could be taken to comply with them. This code helps to plug that gap.

2

How does the DPA apply to information processed online?

- The DPA applies to the 'processing' of 'personal data'. 'Processing' has a very broad meaning and includes everything that happens to personal data collected online.
- The DPA defines 'personal data' as data which relate to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.
- In the Information Commissioner's view, personal data is being processed where information is collected and analysed with the intention of distinguishing one individual from another and to take a particular action in respect of an individual. This can take place even if no obvious identifiers, such as names or addresses, are held.
- A practical difficulty arises when collecting information online because non-obvious identifiers, such as cookies or IP addresses, are linked to a device rather than a particular user. In many cases a device will have multiple users, for example a shared household PC. This may make it impossible to tell whether the information obtained is about a single user or a group of users.

Example

A single household PC may have different family members using it under the same login identity. As a result, the IP address and cookies cannot be connected to a single user. Therefore it is unlikely that this information will be personal data. However, if each family member logs in separately, then any online activity will relate to that particular login identity. This will mean that the cookies used are more likely to be personal data. An IP address is only likely to be personal data if relates to a PC or other device that has a single user.

- When you cannot tell whether you are collecting information about a particular person, it is good practice to treat all the information collected as though it were personal data. In some cases the information will be personal data and the DPA will apply to it. In particular, compliance would involve:
 - keeping the information secure;
 - protecting it from inappropriate disclosure; and
 - being open about how the information is being collected and used.



- The Information Commissioner recognises the practical and sometimes insurmountable difficulties in complying with all aspects of the DPA in respect of non-obvious personal identifiers. In particular he recognises the security issues that may be involved in trying to give an individual subject access to information linked to non-obvious identifiers. He will not necessarily enforce the right in this context unless there is a genuine risk to an individual's privacy if he fails to do so. This issue is explored in more detail in section 6 - Individuals' rights online.
- The Information Commissioner also recognises the practical difficulties in attempting to gain an individual's consent as a means of legitimising the processing of non-obvious identifiers. In most cases the DPA provides alternatives to this.
- Special restrictions apply to the processing of 'sensitive' personal data, such as information about a person's health or political opinions. There may be no alternative to obtaining the individual's consent in order to legitimise the processing of such information.
- Some online content is displayed without any personal data being processed, for example where the same content is displayed to everyone who visits a website. In such cases the rules of data protection do not apply, although other laws or standards may do.

Further information about personal data can be found in our guidance note **A quick reference guide – What is personal data?** and in our more detailed Technical guidance note on determining what is personal data, these are at:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/what_is_data_for_the_purposes_of_the_dpa.pdf

Responsibility for data protection

- The 'data controller' has ultimate responsibility for complying with the DPA. Online, it is possible that a number of data controllers, and possibly 'data processors' working on their behalf, will act together to deliver content or services. Organisations should establish which of them has legal responsibility as a data controller.

Example

A shopping website may allow payments to be taken online via a company which specialises in online payment methods.

The customer may have an account with the website, which means it will be the data controller for that personal data e.g. name, address and shopping history with that website. The customer will often have a separate account with the payment company, which will hold details such as bank account number and credit / debit card details in order to facilitate payment to the website. That company will be the data controller in relation to that set of personal data.

It is important for each of these parties to be clear about what personal data they are responsible for in case, for example, a customer wishes to exercise their rights under the DPA.

Further guidance can be found in the rights of individuals section of **The Guide to Data Protection** which is available at:

http://www.ico.gov.uk/for_organisations/data_protection_guide/principle_6_the_rights_of_individuals.aspx

- It is good practice for organisations to work together to ensure that members of the public, who may be unaware of which organisations are involved and how, are treated fairly. This includes explaining to the public who will use their information and how. The website publisher must take on this role in respect of its own information collection and any collection carried out by third parties via its website. However, the third parties still have their own legal obligations under the DPA.
- If there is evidence of a breach of the DPA, it is the data controllers involved that could be subject to enforcement action or prosecution. Legal responsibility is a matter of fact that the Information Commissioner will establish in the circumstances of the case.
- Where a data controller uses a data processor to provide services on its behalf, there must be a written contract in place ensuring that appropriate security is maintained. This means that the security must be as good as, or exceed, the data controller's own standards, which must in turn be appropriate.

Collecting the right personal data

The DPA says that personal data can only be collected where this is 'necessary'. This means that you must not collect personal data too early in your relationship with someone. It is bad practice to collect personal details like names and email addresses just to let someone look at your website. Individuals may find it intrusive and inappropriate to be asked to provide their details too early on.



- Once an individual starts to interact with a service provider, for example by asking for details of their pension entitlement, or requesting details of a loyalty scheme, it becomes much easier to justify collecting relevant personal data.
- It is good practice to be clear about which information individuals have to provide in order to get the services or goods they have requested and which information they can choose to provide - for example information used to carry out market research. Individuals must not be misled about their choices or about how their information will be used.
- Take care when using template forms provided by a third party supplier. There is a risk of collecting unnecessary information, where a field on the form is inappropriately marked 'mandatory'. This is a breach of the DPA and can annoy individuals because they are being asked for information that is excessive or irrelevant.
- If you are buying an electronic form, it is good practice to ensure that the fields on it correspond with your actual business needs. Ideally, you should use forms that you can tailor to your own needs, for example by removing certain fields or specifying whether their completion is mandatory or optional.

Retaining personal data

- It is good practice to check periodically whether you need all the information you have been collecting, for example by carrying out an audit. If you have information you don't use, you should stop collecting it and delete any unnecessary information you have already collected.
- If it is possible to satisfy your business' needs without retaining information in a form that can identify people, you should do so. For example, an IP address could be made less specific by removing its final 8 characters (also referred to as the final octet) so it cannot be linked to a specific device. Partial postcodes instead of full addresses might allow your organisation to plan its services geographically without holding personal identifiers.
- If you are under a legal obligation to keep information for a specific period of time, for example for accounting purposes, the DPA will not prevent you from doing so. It is good practice to find out what these legal obligations are and establish a retention schedule in line with them. The National Archives has produced guidance on retention schedules which can be found at:

<http://www.nationalarchives.gov.uk/recordsmanagement/retention-disposal-schedules.htm>
- If someone objects to you holding information about them and asks you to delete it, it is good practice to do so where possible. It is acceptable to keep a record of objectors in a suppression list so that you do not contact them again.

- Individuals have a legal right to require you to stop processing their personal data where this is causing, or is likely to cause, substantial damage or substantial distress and is unwarranted.

Keeping personal data secure

- It is good practice to build in security and privacy protection from the very start. Establish clear roles and responsibilities. Undertake risk assessments and identify where your systems and processes may be vulnerable to threats. If you need it, seek professional advice as to how to deliver electronic services securely.
- Know what personal data you collect and store and who has access to it. It is good practice to keep a record of where the information is stored and to keep track of how your organisation collects information e.g. through email, websites and from other sources.
- It is good practice to ensure that when a member of staff leaves your organisation their access to personal information is withdrawn, for example by recalling mobile storage devices and revoking access permissions.
- If your site offers auto-completion facilities for forms and passwords, it is good practice to notify users if this could leave them vulnerable, for example if their mobile device or laptop is stolen. However, ultimately users have a role to play in protecting themselves online, for example by adjusting the auto-complete settings on their browser or on a website they visit. Auto-completion can present a particular risk where an individual's payment card details have been retained for 'auto-fill' purposes. This may mean not offering auto-completion in certain contexts - e.g. on password fields for authorising payments.
- Review your security arrangements on a regular basis. Make sure your technical protection is up to date. Install anti-virus software and keep it updated. Install security patches as soon as they become available to you.
- If you no longer need personal data, make sure you dispose of it securely.
- Assess the risks of a security breach and its potential harm to individuals. Have a plan in place for dealing with security breaches. It is good practice to report major breaches to the Information Commissioner. Further guidance on the notification of serious breaches is available at:

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf
- Allow your staff to access only the information they need to do their job. Make sure each user has appropriate access permissions and have secure access controls in place.

- Train your staff in security procedures on a regular basis so they know what is expected of them. Make sure they are aware of any sanctions that might be used against them if they misuse personal data.

Telling people what you are going to do with their personal data

One of the primary requirements of data protection law is to ensure people are aware of how information collected about them will be used. In many cases this will be straightforward, for example where a customer provides contact details to a local authority so he or she can be included in a residents' parking scheme, or where someone provides their name, address and payment details so that goods can be purchased and despatched.

Sometimes the use of personal data that occurs online is more complex than this, and many individuals may not expect or understand the way their information is used. It is good practice to make a thorough assessment of the way the information you collect is used and to ensure your privacy notice reflects this.

It is particularly important to make special effort to explain the sorts of information analysis that people are unlikely to be aware of because it happens 'behind the scenes' and may use techniques they are not familiar with. If, for example, personal data is going to be used to offer targeted pricing – i.e. offering the same goods to different people at different prices, depending on their previous online behaviour - then this should be explained to them.

When you draft a privacy notice you should make sure it has sufficient prominence for people to access it easily. It should be written in a way that the people who access your service are likely to understand. It should use font sizes and colours that make the text easy to read. Further guidance on privacy notices is available at:

http://www.ico.gov.uk/for_organisations/topic_specific_guides/privacy_notices.aspx

Collecting information about vulnerable people

By 'vulnerable people' we mean individuals who, for whatever reason, may find it difficult to understand how their information is used. This could be because they are children, have a learning disability or lack technological understanding. Data protection law says that you have to process personal data fairly. This duty applies regardless of the level of understanding of the people you collect information from. You should try to assess the level of understanding of the people your service is aimed at and must not exploit any lack of understanding on their part.

One of the difficulties of providing services online is that very often you will not know:

- who is accessing your service;
- how old they are;
- what their level of understanding is;
- how 'internet savvy' they are; or
- whether they have a disability that affects their understanding.

Even if you collect reliable 'real world' identifiers, such as names and dates of birth, this still doesn't mean you can judge levels of understanding reliably. People could provide false details in order to access services. For example, a child could lie about their age.

Uncertainty over the 'real world' identity and characteristics of those you are dealing with does not mean that you cannot collect personal information about them. However, if your website is targeted at a particular group, for example children, there are some precautions that you should take. The adoption of good practice will help to ensure that you handle the personal data of all those that use your services fairly, but it is especially important when dealing with people who are particularly vulnerable or lack understanding.

Information about children

There are many difficulties when collecting information from children, including determining whether parental consent to data collection should be obtained and, if so, what form it should take. For example:

- In the UK there is no simple legal definition of a child based on age. Even if there was, you might not know the ages of many of the individuals you are dealing with, or be able to rely on the information provided by the child or "adult" as to age.
- Children of a similar age can have different levels of maturity and understanding. Consideration of these attributes, as well as age, will be required to ensure that children's data is processed fairly.
- A resourceful and determined child could circumvent many mechanisms for obtaining his or her parent's consent for the collection of personal data.

Age and understanding

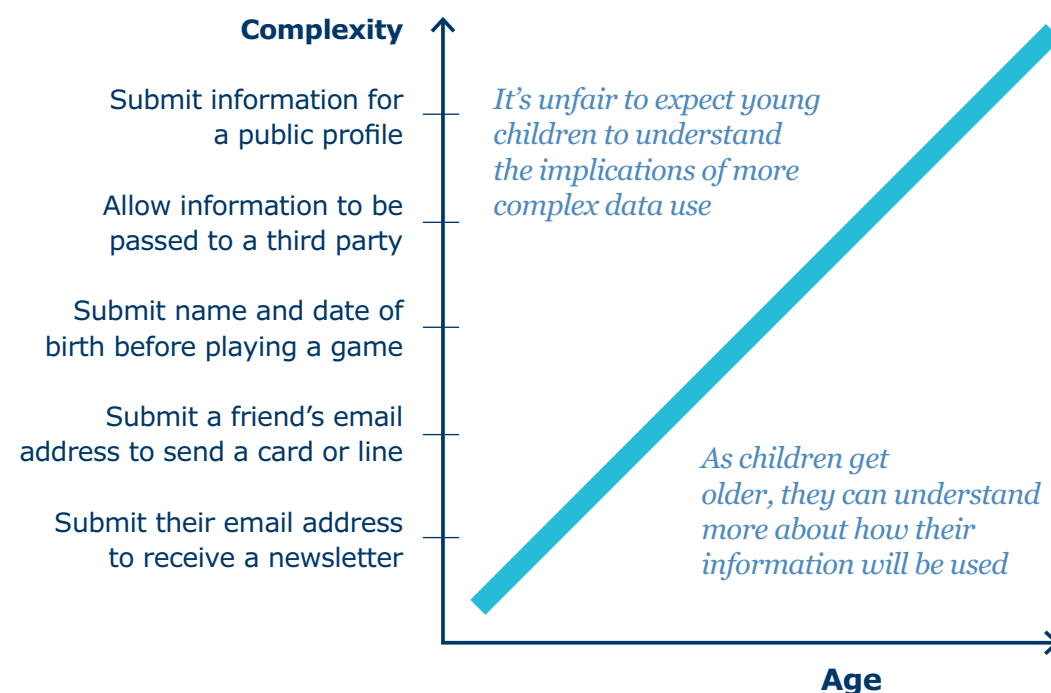
Assessing understanding, rather than merely determining age, is the key to ensuring that personal data about children is collected and used fairly. Some form of parental consent would normally be required before collecting personal data from children under 12. You will need to look at the appropriate form for obtaining consent based on any risk posed to the child. You may even decide to obtain parental consent for children aged over 12 where there is greater risk. This has to be determined on a case by case basis.



Other laws, industry rules or codes of practice may apply to your organisation, for example, restrictions on targeting direct marketing at children under a certain age.



It is clear that certain services are aimed at particular age groups, for example children of primary school age or those in their early teens. It is good practice for the providers of such services to ensure that they only collect personal data in a way that their core audience is likely to understand and that their parents would be unlikely to object to if they knew about it. In short, this means that as complexity increases, it will become more likely that only an older child will have the necessary understanding.



Parental consent



It is good practice to seek parental consent if the collection or use of information about a child is likely to result in:

- disclosure of a child's name and address to a third party, for example as part of the terms and conditions of a competition entry;
- use of a child's contact details for marketing purposes;
- publication of a child's image on a website that anyone can see;
- making a child's contact details publicly available; or
- the collection of personal data about third parties, for example where a child is asked to provide information about his or her family members or friends. This excludes parents' contact details provided for the purpose of obtaining parental consent.

The key issue is to take into account the degree of risk that the collection or use of the personal data poses to the child or to others. This will help you to determine whether parental consent is required and, if so, what form this should take. For example, where minimal information is being collected, such as an email address to register on a site and to ask the child to confirm their age, then asking the child to tick a box to confirm parental consent and sending an email to the parent may be sufficient. However, if the child's photo is to be displayed on a website, you may require a signed consent form or email acknowledgement from the parent even for older children.

Obtaining reliable parental consent can be very difficult. One problem is that it is often the child accessing the service that will be asked to provide their parents' details. This could allow the child to provide false parental details, for example by setting up a bogus email contact address. The promise of a prize or other inducement could encourage resourceful children to do this.

Information about third parties

Sometimes children are asked to provide information about other people, for example their friends or family members. Generally you should only request such information for the purpose of obtaining parental consent. The Committee of Advertising Practice advises that children under 16 should never be asked to provide information about anyone else for marketing purposes. This is good advice, but more generally it is for organisations to assess the level of risk associated with asking a child to provide personal data about a third party. In some cases the risk is low because the information collected is relatively innocuous, for example where a child provides another person's email address to transmit a newsletter and where the address isn't retained or used for any other purpose.

Organisations should consider, on a case by case basis, whether they need to take any additional measures to mitigate any risk posed to individuals whose details have been provided by another person. Where practicable, the organisation should contact the individual to identify itself and to explain what the personal data will be used for. It is good practice to delete the individual's personal data where they request this.

Collecting information about people from the internet

- People may post their personal details in such a way that they become publicly visible – for example through a social networking or recruitment site. Wherever the personal data originates, you still have an overarching duty to handle it fairly and to comply with the rules of data protection. See our leaflet, **Protecting your personal information online**, to read what your customers will be looking out for.
- If you collect information from the internet and use it in a way that's unfair or breaches the other data protection principles, you could still be subject to enforcement action under the DPA even though the information was obtained from a publicly available source.
- It is good practice to only use publicly available information in a way that is unlikely to cause embarrassment, distress or anxiety to the individual concerned. You should only use their information in a way they are likely to expect and to be comfortable with. If in doubt about this, and you are unable to ask permission, you should not collect their information in the first place.



3

Marketing your goods and services online

Organisations have always used information about their customers to market goods and services to them. This is an established practice that customers have come to expect and are generally happy with.

The Information Commissioner receives relatively few complaints about online behavioural advertising. However some individuals are concerned about their online activity being analysed in a way that they consider to be intrusive or inappropriate. These fears may arise partly from a misunderstanding of the technology.

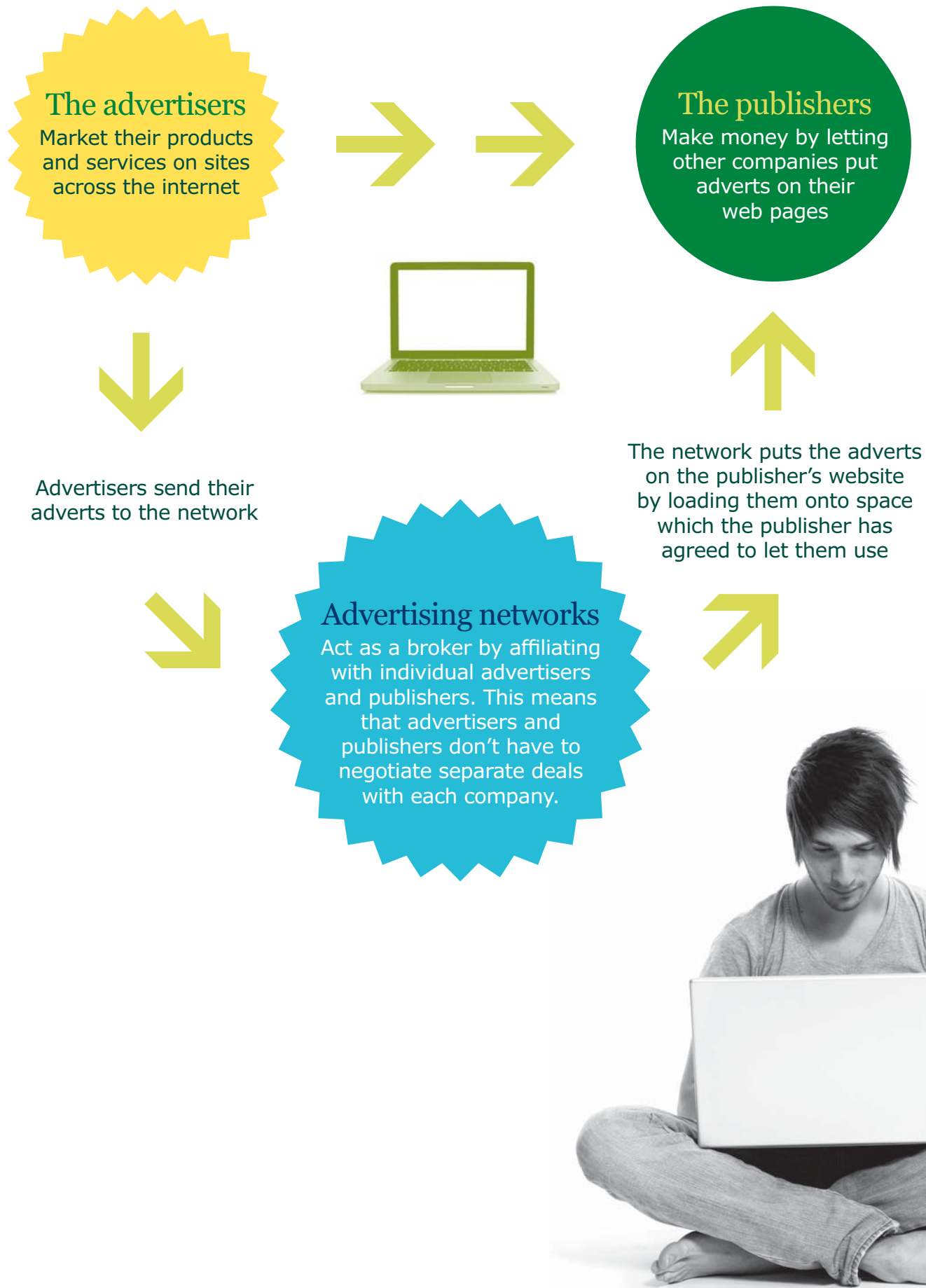
There are two main ways of carrying out online behavioural advertising that involve the processing of personal data:

- 'First party advertising', involves an online retailer marketing its goods by analysing an individual's purchase history, or items they have looked at, and then displaying content, such as a special offer. The offer will typically relate to an item or service that the individual's previous behaviour suggests they might be interested in. This process often involves the use of obvious personal identifiers, such as a name and email address – for example where an individual is logged in to their account.

Example

A customer has an account with a book selling website. The website keeps a record of the books the customer has bought from it on previous occasions. It uses this information to advertise similar types of books which the customer may also be interested in buying. For example, a customer who has bought science fiction novels previously may receive adverts or 'suggestions' for others books of this type.

How online marketing works



Non-targeted marketing

Networks which aren't using targeting rotate random adverts around different sites, so they aren't necessarily relevant to the publisher or the user.

Contextual marketing

Some networks use contextual marketing. They use programs which analyse the content of publishers' sites, and match them with adverts from companies who have chosen to link their adverts to that content.

Contextual targeting is more likely to result in adverts for products which are related to the content of the page the user is viewing.

Behavioural targeting

Behavioural targeting uses information linked through cookies to create a profile of a user. The user is matched with a broad profile, and they are sent adverts which are likely to interest them.

The cookie records which affiliated sites have been visited. It might also record location, and past searches.

- 'Third party advertising' usually involves a third party placing a cookie on a device in order to recognise when an individual visits a website, and then associating particular interests inferred from the individual's web-browsing history with that cookie. The third party typically works under contract to a number of website publishers, from whose sites the browsing data is collected and then processed. In cases like this, the third party will typically not hold any obvious identifiers and will be unable to link the information it holds to an individual's 'real-world' identity. However, the information the third party collects and uses to infer interests may still be indicative of a particular individual's online activity and may still involve categorising an individual, along with other individuals, according to their inferred interests. The end result of this process is that particular content is displayed to particular individuals, depending on the 'score' that is associated with their inferred interests. Allocating the score and using it to target advertising involves the processing of personal data and the DPA applies. However, using personal data in this way is not intrinsically unfair or intrusive, and the DPA provides various options for processing this information legitimately – i.e. there are alternatives to consent. Further guidance about the various options is available in 'The conditions for processing' section of **The Guide to Data Protection**.
- In the case of third party advertising, a website publisher uses a third party to carry out targeting on its behalf. The relationship between the two parties can take different forms. In some cases the publisher will retain overall responsibility for the processing of personal data, with the third party acting purely on the publisher's instructions. In others, the third party will retain control over how the personal data is processed, meaning it will have its own data protection responsibilities.
- There can be privacy advantages in third party advertising, in that the third party will usually not have access to the obvious identifiers, e.g. registration data, that a 'first party' site owner may hold in respect of its own customers.
- However content is delivered, it is good practice for the organisations involved to work together to ensure that overall standards of fairness are maintained. This is particularly important given that many individuals will not be aware that a number of organisations are involved in the delivery of content to them.

See www.youronlinechoices.co.uk. This site includes the Internet Advertising Bureau's good practice principles.

Marketing choices

- It is in an organisation's interests to be open about the techniques it uses and to make clear the options people have to opt out of marketing, including the use of web browser settings. This allows individuals to make an informed choice about whether to use a particular service. Being open may also help them to understand and accept the analysis of information that underpins their online activity, and which may support the services they rely on. Providing clear opt-outs also allows people to exercise control when using your services online.
- It is good practice to give individuals as clear and simple an explanation as possible of what happens when they access your service, how information about their visit is collected and analysed and the result of this – e.g. being served an advertisement for a particular product. The explanation should be given due prominence and be expressed in terms you think most visitors to your site could understand. A more visual or 'diagrammatic' approach can be a good way of explaining how the technology works. Further information about explaining your collection and use of personal information is available within the ICO's Privacy Notices Code of Practice which is available at:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf
- Some individuals may want to visit a website without any record of their online behaviour being retained. Therefore it is good practice to provide a simple means of disabling the targeting of advertising using behavioural data. It is a legal requirement under the Privacy and Electronic Communications Regulations (PECR) to tell the individual when information is to be stored on their equipment, for example in the form of a conventional cookie, a Local Shared Object or flash cookie, and to give them the opportunity to refuse this.
- It is good practice to offer users relevant advice about how they can use their web browser settings, or the choices offered on the website itself, to exercise choice over the extent to which they preserve their online anonymity, for example by ensuring that information identifying them is erased at the end of a session.
- Where the use of cookies is strictly necessary for the provision of goods and services, organisations are under no obligation to provide the service to individuals who refuse the necessary cookies.





The ICO's guidance on the Privacy and Electronic Communications Regulations (PECR) explains the rules relating to the use of cookies.

http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/guidance_part_1_for_marketers_v3.1_081007.pdf

There is a possibility that these rules will change within the near future as a result of the UK's implementation of Article 2 of EU Directive 2009/136/EC. If they do we will update our guidance.

Using sensitive information

Sometimes people will access sensitive content on the internet, for example on a website run by:

- a political party;
- a debt counselling company;
- a sexual health clinic;
- an advice service for ex-offenders; or
- a religious group.

The DPA defines certain categories of personal data as 'sensitive'. Although the definition in the Act serves as a useful starting point, organisations must make their own assessment of sensitivity, based on the nature of the information they publish and individuals' likely attitude to it.

The threshold for processing sensitive personal data to deliver advertising is high. The DPA provides no obvious alternative to obtaining the individual's explicit consent to the use of sensitive personal data for this purpose.

The key to preventing distress or embarrassment is to ensure that there is a facility on the website itself for obtaining explicit consent – i.e. an indication of the individual's choice – for the serving of first or third party advertising based on the website's sensitive content.

Particular problems could arise when a visit to a sensitive website leads to ads related to its content being displayed on a different website. Where a device, for example a home PC, is shared between family members, this could allow one person to deduce that another has been accessing websites about, say, a sexual health problem. The key to managing this is for the publisher of the website to obtain explicit consent for the advertising in the first place.



Privacy choices

By 'privacy choices' we mean the options that people are given on web browsers or websites that allow them to exercise a degree of control over how their online personal data is used.

For example, they allow people to choose whether to accept cookies, whether a record of their previous browsing activity (i.e. 'history') is kept, or whether the information needed to complete a form automatically is retained. These choices also allow users to enable features that may allow them to make better use of the internet, for example the provision of 'recommendations' based on previous purchasing history or of content linked to their interests or geographical location.

Browsers and websites

The relationship between the software that people use to access the internet, and the websites they choose to visit, is crucial for data protection compliance.

Browser software – such as Firefox, Internet Explorer or Safari – allows individuals to go online and to manage their online settings, including their privacy preferences. The companies providing the browser may collect non-obvious identifiers for analytical purposes, but do not normally collect obvious personal identifiers, unless they offer additional services such as personalised homepages or webmail.

Browser preferences are important for two main reasons:

- When online, they allow individuals to control their interaction with the websites they visit, for example whether to accept third party cookies.
- When offline, they allow individuals to manage the information stored on their PC or other device, for example their browsing history or the sites stored on their 'favourites'. This can have important privacy implications, particularly where several people share a device.

In so far as the browser supplier processes personal data, it must honour its obligations under the DPA. However, in addition to this, suppliers of browser software have a key data protection role to play, because individuals will generally use their browser to manage their privacy preferences when accessing other organisations' services online. The Information Commissioner therefore encourages providers of browser software to continue to develop simple, easily accessible tools to help individuals manage their privacy preferences.

In reality, many individuals may fail to understand the relationship between their browser and the services they access through it. For this reason, it is good practice for each browser supplier and online service provider to be aware of the privacy management facilities that each offer and to ensure, as far as is possible, that individuals enjoy an appropriate degree of control over their personal data. Online service providers cannot justify unfair or excessive information collection just because individuals have the option to protect themselves against this by using their browser settings.

Default settings

In practice, most individuals do not use the privacy choices available to them. This could be because they do not look for them, cannot find them, do not understand them, or fail to recognise their significance. Alternatively, it may simply be that they expect a basic level of privacy protection without the need for them to exercise what can sometimes be multiple and complex choices. In addition, they may fail to access or read a company's privacy notice.

- It is good practice, therefore, to set privacy defaults in a way that strikes the right balance between privacy protection and functionality. The key to this is to ensure that only necessary, relevant information is collected and that it is used in a way that individuals are likely to expect given the services they have chosen to access.
- The default position should normally be that information is not shared with another organisation, except a sub-contractor, or used for a different purpose – this provides the best degree of protection to individuals who fail to register their own preferences. If defaults are not set in this way, for example where boxes are pre-ticked to allow disclosure, it is good practice to state clearly that users can change their settings and to explain the implications of failing to do so.
- It is good practice to draw individuals' attention to any relevant privacy choices at the time their personal data is collected. This will allow them to make an informed choice as to whether to provide their personal data, and if so, how much to provide and what choices to exercise in respect of its use. It is good practice to give privacy choices prominence and to use language that the individuals your website is aimed at are likely to understand.

Despite an organisation's best efforts to make individuals aware of the privacy choices available to them, many users will continue to pay little, if any, attention to them. Organisations must recognise this and remember that they remain under a duty to collect and use personal data fairly. It is good practice therefore to set privacy defaults to reflect the likely wishes and expectations of the individuals you deal with and the nature of your business.

If a noticeable number of individuals are altering their privacy settings from the default position to require more privacy, this could mean that the default is set inappropriately and ought to be amended to correspond more closely with their wishes. Where possible, it is good practice to monitor this and make adjustments as necessary. It is also good practice to monitor complaints and 'chatter' on the internet concerning your organisation in order to detect privacy concerns early.

Respecting individuals' choices

Some websites, for example social networking sites, allow service users to control who has access to their personal data. Where individuals have control over this, their choices must be respected. If there is an intention to change the way a service is run, resulting in the extent of access to personal data about service users being changed, it is good practice to inform users of the proposed change and to obtain their consent for this.

Similar issues can arise when an organisation decides to launch a new service, for example where a company providing a webmail service starts to provide a social networking site. It is bad practice to assume that the new service can be populated with personal data from the original service. Individuals' original choices about the use of their personal data, and access to it must be respected. It is unfair to populate a new list of social networking contacts from an existing email address book, for example, if this results in the individual's preferences concerning access to their personal data being overridden without clear consent. Again, where a change of this sort is envisaged, you must inform users and to obtain their consent for this.



5

Operating internationally

The DPA says that personal data transferred overseas shall enjoy an adequate level of protection. The DPA's overseas transfer rules can be difficult to comply with online because:

- UK organisations may collect and use personal data about citizens of other countries;
- overseas organisations may collect and use personal data about UK citizens;
- UK organisations may use equipment or subcontractors overseas to carry out their business;
- overseas organisations may use equipment or subcontractors in the UK to carry out their businesses.

Even if your company is based in the UK and only offers services to people in the UK, your use of internet-based computing may still involve transferring personal data overseas.

The DPA says organisations established in the UK, or non-European ones using equipment in the UK, must comply with UK law regardless of where the personal data originates from. However, when collecting, storing, using or distributing personal data across international borders, organisations in the UK and elsewhere could be required to comply with several different sets of rules. This can raise practical compliance difficulties for organisations:

- you may not know where information you are responsible for is being processed at any particular time; or
- you may not know where people you are collecting information about are situated, what privacy standards they might expect, or what the law in their country says.

Given the practical problems that arise from these territorial issues, a good practice approach is particularly useful.

The principles of the DPA have international roots and are similar to those found in other countries' laws, within and beyond the European Union. Compliance with the principles should generally serve as a reliable foundation for international compliance, despite variations in national laws. However, you may need to take different, or additional, measures, depending on the people you aim to collect personal data about, the nature of the service you are providing and the regions at which you are aiming your services.

When aiming to collect personal data from people in a particular country or countries, it is good practice to try to understand any relevant cultural values and expectations that could lead to your processing of personal data being considered to be inappropriate or intrusive. In practice this can be difficult, especially if your service is not targeted at a particular group or territory. If in doubt, advice should be sought from experts in the countries you are targeting.

It is good practice to be as open as you can with your customers about where any processing of personal data is taking place and the likely consequences of this, if any. Note, though, that the DPA does not give individuals a right to insist that their personal data is only processed in one country and not in others.

Cloud computing

The use of cloud computing, or 'internet-based computing', involves an organisation using services – for example data storage – provided through the internet. Organisations using these services might not store the personal data they are responsible for on their own equipment. Therefore organisations may not be certain where the personal data is being processed. Complex chains of contractors and subcontractors mean that, in addition, organisations may not be certain who is processing personal data on their behalf. The DPA does not prohibit the overseas transfer of personal data, but it does require that it is protected adequately wherever it is located and whoever is processing it. Clearly, this raises compliance issues that organisations using internet-based computing need to address.

Your use of an internet-based service must not lead you to relinquish control of the personal data you have collected, or expose it to security risks that would not have arisen had the data remained in your possession in the UK. There must be a written contract in place. This can be an electronic one, requiring the internet-based service provider to only act on your instructions and to have a level of security equivalent to yours.

It is good practice to encrypt the data prior to it being transferred to the online services company. This should render the data useless to any hackers and snoopers without the key, regardless of the jurisdiction it is in or who is processing it. Modern techniques increasingly allow processing operations to be carried out whilst maintaining the security and integrity of the data.





Despite the potential problems, there can be advantages for your company's back-up and security procedures if multiple copies of personal data are held in multiple locations, as can happen when using internet-based computing. This can minimise the effect of a serious IT failure on a single site or the theft of a server, for example.

It is good practice to conduct a risk analysis before contracting with an online services company, or with other contractors. This might include the following questions:

If your organisation is thinking of using an internet-based computing company:

- Can it confirm in writing that it will only process data in accordance with your instructions and will maintain an appropriate level of security?
- Can it guarantee the reliability and training of its staff, wherever they are based? Do they have any form of professional accreditation?
- What capacity does it have for recovering from a serious technological or procedural failure?
- What are its arrangements and record regarding complaints and redress – does it offer compensation for the loss or corruption of data entrusted to it?
- If it is an established company, how good is its security track record?
- What assurances can it give that data protection standards will be maintained, even if the data is stored in a country with weak, or no, data protection law, or where governmental data interception powers are strong and lacking safeguards?
- Can it send you copies of your information regularly, in an agreed format and structure so that you hold useable copies of vital information at all times?

If the answers to any of these questions raise concerns about a company's ability to look after the information you are responsible for, you should not use the provider concerned and should seek alternatives.

If you are considering using a provider that may not be familiar with UK law and best practice, but otherwise seems to maintain appropriate standards, send them this and other relevant guidance so they can review it and satisfy you that they maintain adequate standards.

If your company is offering online services to other organisations, can you:

- provide written guarantees about your security arrangements?
- guarantee that data will only be processed in accordance with your clients' instructions, e.g. that it will not be retained for longer than instructed?
- guarantee that your staff are trained and vetted to suitable standards, wherever they are based?
- explain your capacity to deal with serious technological or procedural failures?
- explain your complaints and redress procedure e.g. do you offer compensation for loss or corruption of clients' data?
- explain the facilities you offer to maintain high data protection standards, even if you store data in a country with weak, or no, data protection law, or where governmental data interception powers are strong and lacking safeguards?
- provide your customers with copies of their information regularly, in an agreed format and structure, so that they hold useable copies of vital information at all times?

If you cannot answer these questions to your potential clients' satisfaction, you will be at a competitive disadvantage. If you comply with any relevant standards – e.g. security – make this clear on your website.

For information about overseas transfers, see:

http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx

Further guidance is available in **The Guide to Data Protection** at:

http://www.ico.gov.uk/home/for_organisations/data_protection_guide.aspx



6

Individuals' rights online

The DPA gives individuals certain rights over their personal data. These include:

- the right of access to personal data held about them;
- the right have personal data corrected if it is wrong; and
- the right to stop personal data being used for direct marketing.

Individuals should also be aware of who is processing their personal data, what it is being used for, who it may be disclosed to and what the source of the data is.

Organisations are only required to give individuals the rights that the DPA provides them with. However, it is good practice for organisations operating online to use their technology to give individuals easy ways of exercising their rights. They should also find helpful ways of explaining how information is obtained, used and disclosed. This becomes more important as online information systems become more complex.

Access to online information

Obvious identifiers

The usual rules apply when giving access to personal information linked to obvious identifiers, such as information filed under a customer's name and address or a patient's NHS number, regardless of whether the individual accesses the service online or in more traditional ways.

Where individuals access your services online, it is good practice to also allow them online access to their personal data. Although this may not always be possible, in many cases it will be. The use of metadata, or other flagging, can help to determine the data that can be released automatically in response to a request and that which needs prior assessment by the data controller.

Although the DPA allows a fee, usually £10, to be charged for granting subject access, it is good practice to waive the fee, or to reduce it, when the online accessing of information incurs no additional costs for the data controller.

Although the DPA gives the data controller up to 40 days to comply with a request, it is good practice to give access sooner than this, or in real time, where the technology allows this.

If you are going to grant individuals online access to their personal data, you must be sure of the identity of the person making the request. This could be done, for example, by giving access when signed in to a password protected online account.

Non-obvious identifiers

Although the collection and use of non-obvious identifiers can constitute the processing of personal data, there are significant practical difficulties in granting subject access to information of this sort.

There will be many cases where an organisation only holds non-obvious identifiers and either has no interest in, or no certainty of, the 'real world' identity of an individual. Whilst these identifiers may be personal data, there is a major privacy risk inherent in granting subject access to information that is only logged against a non-obvious identifier such as an IP address or cookie, rather than against other information more clearly related to a particular individual. The problem arises because the information held is linked to the device used to go online, rather than directly to the person using it. In reality this means that the organisation holding the information may not be able to determine with any degree of certainty whether the information requested is exclusively about the person making the subject access request, or about a group of people using the same device to go online. In many cases, it is difficult to envisage what practical measures the organisation holding the information could take to satisfy itself on this point.

Where a reliable link between the subject access applicant and the information held cannot be established, and where, therefore, there is an obvious privacy risk to third parties, the Information Commissioner would not necessarily seek to enforce the right of subject access unless there is a genuine risk to an individual's privacy if he fails to do so. However, this information still needs to be carefully protected because of the risk that otherwise someone may, with greater or lesser certainty, be able to infer something about a particular person – for example if it was published and combined with information held by other organisations.

Where an organisation does hold details of the 'real world' personal identity of the subject access applicant, and can be satisfied with a reasonable degree of certainty that the applicant in question is responsible for the activity to which the requested information relates, the Information Commissioner would expect subject access to be given. This may be the case where an individual has provided their 'real world' personal details in order to register for an online service.



Working together to help the public

It can be difficult for people to understand who is responsible for content they see online – for example where a company's website hosts third party content. Many individuals will assume that one organisation delivers all the content they see on a website, when in fact several different organisations may be responsible.

It is good practice for the company with primary responsibility for the website – the website publisher - to act as a single point of contact for issues relating to the processing of personal data, even if it is not legally responsible for all aspects of this. At least, the website publisher should help members of the public to contact the third party should they have concerns or questions about the collection of information or the content displayed to them. This does not mean that the website publisher takes on legal responsibility for all the processing of personal data carried out through its site.

Sorting problems out

- It is good practice to make it easy for individuals to contact you if they have a problem with their personal data. You could do this by displaying your contact details, or a link to them, on your home page or by including them in your privacy notice.
- Organisations operating online should work towards making it easy for individuals to find out who is responsible for an ad, for example by clicking on it.
- It is good practice to give individuals online facilities for changing their details or preferences, or accessing and correcting their information.
- It is bad practice to make people contact you by letter or telephone if you provide services to them online. It is also bad practice to expect individuals who have reached your homepage to follow a large number of links or to navigate a number of different pages before they can access your contact details.
- It is good practice to make it easy for people to be able to exercise their preferences, for example in relation to what marketing they are willing to accept, by displaying a clear opt in/opt out at the point when you collect their personal data, or when they register for your service. You should also make it easy for people to change their preferences at a later date.
- If individuals choose to unsubscribe from your service, close an account or request that their information be deleted, it is good practice to meet these requests, or help individuals to do this themselves, as soon as possible, unless you have a compelling business need or are under a legal obligation to retain the information. It is acceptable to keep a record of objectors in a suppression list so that you do not contact them again.

- It is good practice to make it clear to people what will happen to their information when they close their account – i.e. if it will be deleted irretrievably or simply deactivated or archived. Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it.
- If you offer users the option to delete personally identifiable information uploaded by them, the deletion must be real i.e. the content should not be recoverable in any way, for example, by accessing a URL from that site. It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not.
- It is good practice to monitor customers' complaints and queries about the processing of their personal data and to take any remedial action as soon as possible. This will help you to ensure that the way you handle personal data is fair and is in line with your users' expectations. Further information on individuals' rights, and guidance to help you to comply with them, is on the ICO website www.ico.gov.uk



7

Things to avoid

These are some practices that you should avoid, and which could result in the ICO taking enforcement action against you:

- Being secretive or misleading when you collect personal data. People will not trust you and will go somewhere else. This could be a breach of the first data protection principle.
- Not being clear about the purposes for which you use or disclose personal data, or changing these purposes without consent once the personal data has been collected. This could be a breach of the second data protection principle.
- Collecting personal data you don't need or collecting it too early in the process. People do not like organisations that collect too much information about them. This could be a breach of the third data protection principle.
- Keeping records about people that are inaccurate or out of date. Everyone expects their information to be correct. This could be a breach of the fourth data protection principle.
- Collecting personal information and keeping it for longer than you need to in a personally identifiable form. People do not like too much information to be retained about them. This could be a breach of the fifth data protection principle.
- Not respecting individuals' rights over the information you hold about them, for example denying access to personal data. This could be a breach of the sixth data protection principle.
- Having poor security and failing to maintain responsibility for the personal data you collect. Everyone expects their information to be looked after properly. This could be a breach of the seventh data protection principle.
- Failing to ensure the personal data you are responsible for is protected properly if it is transferred overseas. This could be a breach of the eighth data protection principle.



Annex: Preserving privacy online

The following techniques can help you to:

- find alternatives to collecting personal data in the first place;
- avoid holding personal data in a form that identifies people explicitly;
- only process the personal data you need; and
- control the use of, and access to, personal data.

Find alternatives to collecting personal data in the first place

- Where possible, let people access some or all parts of your service anonymously. Don't assume you need to collect personal data about everyone that accesses your service.
- Where someone just wants to look at your website without carrying out any sort of transaction, work out whether you really need to make them register, sign in or provide their personal details.
- Many people will want to access your service anonymously, and may be suspicious if you ask them for their details where there is no obvious justification for this.

Avoid holding personal data in a form that identifies people explicitly

- Pseudonyms are a way of identifying an individual through an alternative digital identity. Pseudonyms can allow individuals to identify themselves to other users of an online service, or to personalise an account, without revealing their 'real world' identities.
- Blind signatures are a type of digital signature that allow people to authenticate their identity to a high degree without disclosing their actual name or other personal details.
- 'Federated identity management systems' involve an independent third party, trusted by both the individual and the service provider, keeping the 'key' that links a digital pseudonym to a real-world identity. This allows an individual to authorise a transaction without the service provider being provided with their 'real world' identity or payment card details, for example.

Only process the personal data you need

You should only process the personal data you need to provide your service. This means you should only collect what you need and shouldn't retain it in a personally identifiable form unless this is necessary.

For example:

- Do not retain complete IP addresses if you can carry out your analytics using only partial ones, for example to determine the broad geographical location of visitors to your website. Set up a retention schedule for complete IP addresses.
- Do not collect complete names and addresses if, for example, you only need a person's postcode to tell them where their nearest branch of your store is. Don't retain this information once you have answered the individual's enquiry. If you want to retain the information, for example to decide whether to open a new store in an area from which you receive a lot of enquiries, only retain partial postcodes.

Control the use of, and access to, personal data

- A 'sticky privacy policy' is a set of 'permissions' attached to a set of information. It allows a person's preferences in relation to their personal data, for example whether it can be used for direct marketing, to be respected even if the information moves from one organisation to another. This should ensure personal data is processed in line with individuals' wishes even though it has moved across a complex information system.
- Encryption can protect your information whilst being stored or transferred to another organisation. It can be particularly useful when taking or transmitting payment details or other sensitive information. It can also ensure that personal data has not been compromised, by proving that the information sent is the same as the information received.

Further guidance can be found at:

http://www.ico.gov.uk/news/current_topics/privacy_by_design.aspx



Glossary

Ad network – a firm that connects advertisers to websites that want to host advertising. As well as paying websites, they may also pay software firms, who show adverts when their software is used or website visited.

Ad server – a web server that stores adverts for use online and delivers them to website visitors.

Advertising agency - a firm that may design advertisements; book advertising space/time; plan/conduct advertising campaigns.

Anonymised information – where information which could be used to identify a single person is encoded or removed to protect individual privacy.

Back-up - reserve copies of data made and kept in case the original is lost.

Behavioural advertising – targeting selected advertising at individuals to increase likelihood of product take-up. Based on information collected about individuals which often derives from which websites they have visited or the searches they have made.

Browser – software that acts as a vehicle to access and interact with information and services on the internet.

Browser provider – a firm that provides software which can be used to access the internet.

Cookie - a text file created on a computer when its user first visits certain websites. It stores information the website uses during visits to it e.g. to provide behavioural advertising.

Cloud computing – online or internet-based computing, where services and information are provided over the internet, without the need for certain hardware or software at the physical point of access.

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

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

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

Default settings – preset controls of hardware or software, usually determined by the manufacturer or vendor.

e-government – provision of government services and facilitation of interaction between government and citizen or business by electronic means (e.g. making enquires, applying for services such as benefits or paying taxes online etc.).

Encryption - conversion of data into a code so it cannot be read without a key.

First party advertiser – a firm that advertises its products and services on its own website.

Hacker - a person who enters computers or networks without permission, often for malicious purposes.

Internet Service Provider (ISP) – a firm that provides its customers with access to the internet.

IP address - a unique sequence of numbers which identifies an online device.

Metadata – descriptive information about a set of data (e.g. title, date created). Sometimes described as data about data.

Online Behavioural Advertising (OBA) provider – a firm that links online advertising with its intended audience, by targeting internet users who display certain online habits/interests e.g. visiting travel websites.

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

- a. from those data, or
- b. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

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

- a. organisation, adaptation or alteration of the information or data,
- b. retrieval, consultation or use of the information or data,
- c. disclosure of the information or data by transmission, dissemination or otherwise making available, or
- d. alignment, combination, blocking, erasure or destruction of the information or data.

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

- a. the racial or ethnic origin of the data subject,
- b. his political opinions,
- c. his religious beliefs or other beliefs of a similar nature,
- d. whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- e. his physical or mental health or condition,
- f. his sexual life,
- g. the commission or alleged commission by him of any offence, or
- h. any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Social networking – expanding one’s social or business contacts via the internet, especially specific websites such as Facebook, LinkedIn, MySpace etc. Members create personal pages on such a site giving information about themselves and communicate with other people (frequently previously unknown) via such websites.

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

Third party advertiser – an advertiser who buys space on others’ websites to advertise its products.

Virus - malicious computer code that replicates itself infecting files and spreading across computers causing nuisance and harm. They can also be used for criminal activity.

Website publisher – a person or organisation that places a website on a web server, making it available over the internet. (This is not necessarily the same person or organisation that creates the content to be uploaded onto the web server.)

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

www.ico.gov.uk

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

July 2010

ico.

Information Commissioner's Office

Upholding information rights