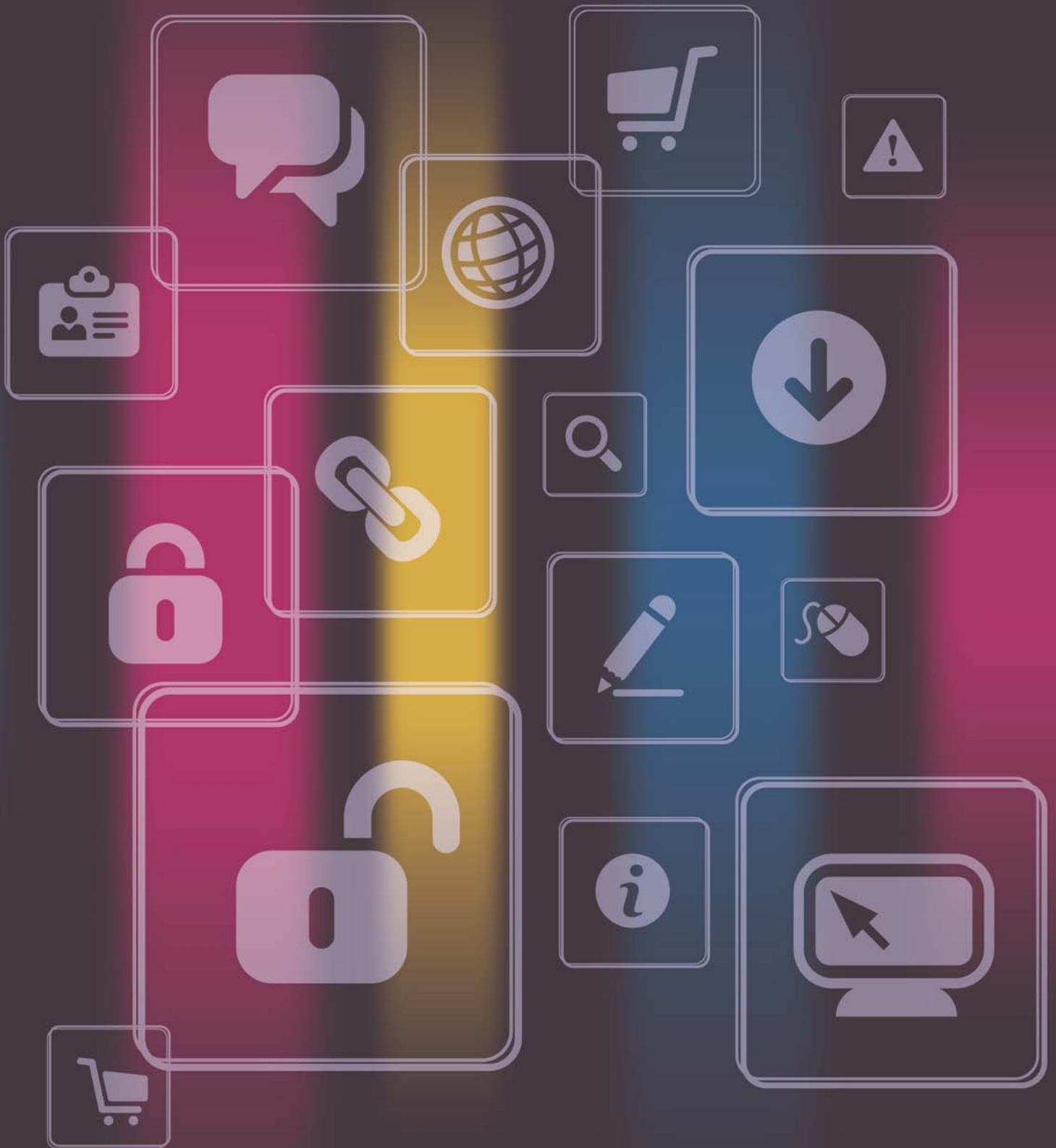


Personal information online code of practice Consultation document





Contents

Introduction to consultation	1
1. About this code	2
2. Who is this code aimed at?	2
3. The code's status	2
4. Benefits of the code	3
5. How to use the code	3
6. What information does the code apply to?	4
7. Data protection online	6
8. Marketing your goods and services online	10
9. Privacy choices	12
10. Operating internationally	13
11. Individuals' rights online	16
12. General consultation questions	19
13. How to respond to the consultation	21





Information Commissioner's Office



Information Commissioner's Office

Introduction to consultation

The online universe is expanding and developing rapidly. New technologies and services are transforming the way we do business. The increasing take-up of social networking, email, e-commerce and e-government reflects our growing dependence on the internet as a means of conducting business, whether personal or professional.

The internet offers great possibilities for convenience and for new experiences, but it can also present risks. A record of our online activity can reveal our most personal interests. This code explains the privacy risks that can arise and suggests ways of dealing with them by adopting good practice.

This code sets out clear, comprehensive recommendations for handling personal data properly and for giving individuals the right degree of choice and control over it. It should also help all organisations with an online presence to negotiate areas of legal uncertainty by adopting good practice.

The purpose of this consultation is to seek the views of those who will be affected by the new code and to ask for suggestions for improving it.

1. About this code

This code provides good practice advice for all organisations involved in collecting and using personal data online. It covers obvious identifiers, such as individuals' names, email addresses or account numbers obtained, for example, through the completion of an electronic application form. However, it also covers the collection and use of less obvious identifiers, for example information indicating individuals' online activity generated through the use of cookies. The legal implications of collecting these less obvious identifiers can be unclear. We hope that the good practice advice contained in this code will be particularly useful in this context.

We have tried to make the code as technologically neutral as possible, focusing on the nature of the information collected and its effect on individuals, rather than the equipment in use. However, the nature of the technology inevitably affects the way information is processed by it.

The code applies to activities such as:

- collecting a person's details through an online application form;
- creating a personal profile of a website visitor by analysing his or her online activity;
- collecting and using personal data for the purposes of marketing goods and services online;
- using cloud computing facilities to process personal data; or
- profiling individuals for other legitimate purposes.

This code does not apply to information that does not, or could not, identify an individual - for example properly anonymised or statistical information. It does not apply either to activities like displaying the same broadcast-type content to everyone visiting a website, because this does not involve the processing of personal data.

2. Who is this code aimed at?

The code is aimed at all organisations that collect information about people online, for example through their PCs, games consoles, mobile devices or media players, either directly or through the use of a third party. However, it will be of most use to organisations that deliver their services online but do not have access to specialist legal or technical in-house advice. Specifically, the code is aimed at data controllers – those who determine the purposes and manner, in which personal data is processed. However, it will also be of use to data processors – organisations that process personal data on behalf of a data controller.

3. The code's status

The code has been issued by the Information Commissioner under section 51 of the Data Protection Act 1998 (DPA). This requires him to promote good practice, including compliance with the DPA's requirements, and empowers him, after consultation, to prepare codes of practice giving guidance on good practice.

The good practice guidance in this code will help organisations handling personal data to adopt practical measures that will help them to comply with the legal requirements of the DPA. The guidance in this code is based on the legally enforceable principles that lie at the heart of the DPA.

The basic legal requirement is to comply with the DPA itself. Organisations may find alternative ways of meeting the DPA's requirements, but if they do nothing then they risk breaking the law. The Information Commissioner's Office (ICO) cannot take action over a failure to adopt good practice or to act on the recommendations set out in this code.

4. Benefits of the code

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 the information is about.

Specific benefits of adopting the code's recommendations include:

- higher levels of trust and a better relationship with the people you collect information about;
- a competitive advantage - by reassuring the people you deal with that you take their privacy seriously;
- encouraging people to provide more valuable information, because they are confident it will be used properly and kept securely;
- helping you to use new technology in a privacy-friendly way; and
- reducing the risk of queries, complaints and disputes about your use of personal data.

5. How to use the code

Different organisations have different needs, depending on the sort of online services they provide and the sort of information they handle. This code can therefore be used in various ways. For example:

- it can be used as a checklist to evaluate your current procedures;
- its content can be used to improve your existing procedures; or
- it can be used to make sure a new online service is delivered in a privacy-friendly way.

We hope that the code will help organisations to work out their own compliance solutions. However, the ICO will provide additional assistance and guidance, for example if an organisation is developing a system that poses particular privacy risks.

6. What information does the code apply to?

The DPA, and this code, apply to personal data. The DPA defines personal data as data which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. The concept of identification is key here. In the Information Commissioner's view an individual can be identified if his or her behaviour can be distinguished from that of a group of other individuals. This can take place even if no real world identifiers, such as names or addresses, are held.

It is generally fairly easy to determine whether information containing obvious identifiers, such as an individual's name and address, is subject to the DPA. However, in online contexts the situation can be less clear because the form of identification may be less obvious. For example, an organisation might use information generated through the use of a cookie to build up information about individuals' online activity, even though no obvious identifiers, such as names and addresses, are being collected. The use of such techniques can allow information about the visitor to be accumulated in such a way that an indicator of the visitor's online activity, and therefore interests, may be inferred. This information can constitute personal data.

In fact, the use of cookies or the analysis of Internet Protocol (IP) addresses can allow the accumulation of information linked to the device used to go online, rather than its user. However, in many cases information, such as a profile or 'score', linked to a device will, in effect, be about the individual using it. In some cases a number of different people, for example family members, will use the same device to go online and perhaps to access the same websites. This means that it may be extremely difficult in practice to determine whether a single individual, or a number of individuals, is responsible for the online activity carried out through a particular device. Where it is not possible to ascertain this, it is good practice, as far as it is possible, to treat the information collected as though it was personal data. In particular, this would involve keeping the information secure, protecting it from inappropriate disclosure and being open with individuals about how information is being collected and used. However, the Information Commissioner recognises the practical difficulties, sometimes insurmountable ones, in complying with all aspects of the DPA in respect of non-obvious personal identifiers.

Sometimes, it will be more certain that the use of a cookie, for example, leads to the accumulation of information about a particular individual. For example, placing a cookie on a mobile device can lead to a website retaining information about such matters as preferences and browsing history linked to the cookie placed on that device. This is very likely to be personal data because a mobile device, such as a phone, is unlikely to be shared by a number of people and therefore the information stored by the website is likely to reflect a specific individual's online preferences and activities. Similar considerations apply where different cookies are put on a particular device depending on the identity of the user that is logged on to the device at the time. Again, where it is not possible to ascertain whether the information being processed is about a single person or a number of individuals, it is good practice, as far as it is possible, to treat it as if it was personal data – which in many cases it will be.

Even if it is not possible to say with certainty whether the information obtained by placing a cookie on a device is personal data, in many cases a device will be used exclusively by a single person and the information will, therefore be personal data. Determining whether this is the case would require access to information that few organisations could ever have access to. In reality, most organisations operating online will never be able to ascertain whether a particular device has a single user or a number of users. However, this does not mean that personal data is not being processed by them.

Some online content is displayed without any personal data being processed, for example where the same content is displayed to everyone who visits a particular website. In such cases the rules of data protection do not apply, although other laws or standards may do. See for example the [Internet Advertising Bureau's good practice principles](#)

This is a difficult area of the law, and one where, for the reasons set out above, it may not be possible for organisations to ascertain in a particular case whether the DPA applies to the information they collect. In such cases, organisations may need to obtain more expert legal advice before they proceed with a particular activity.

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.](#)

Question 1

Does this section explain clearly what information this code applies to?

Question 2

Have we properly understood the technical issues of collecting personal data online?

7. Data protection online

Who is responsible for data protection?

In some online contexts there can be uncertainty about who the data controller is. In fact, a number of data controllers could be operating in common to provide a particular service, perhaps with other organisations providing services on their behalf. Members of the public may be confused about the relationships and responsibilities involved. There may also be confusion amongst the organisations involved about the respective responsibilities of website publishers, content providers, advertisers, advertising agencies, advertisement networks and technology companies. Where responsibilities overlap, it is good practice for all the organisations involved to work together to establish their respective responsibilities. In particular, they should determine who is the data controller, or controllers, in respect of any personal data being processed. Data controllers should, in turn, ensure that any third party contractors they use are aware of their contractual obligations in respect of the personal data they have been asked to process.

Identifying individuals online

The DPA says that personal data shall not be excessive in relation to the purpose, or purposes, for which it is processed. This means that you must not collect information that can identify a person unless you need to do so. If you can justify collecting personal data, you should only collect what you need. For some online purposes, you may not need to collect obvious identifiers, such as an individual's name and address. For example, the analysis of information obtained through a cookie may be enough to determine how frequently a visitor returns to your website. It is good practice, and is in line with the principles of privacy enhancement, to avoid the collection of obvious identifiers where less obvious identifiers would suffice.

Handling personal data

Those collecting personal data need to comply with all the data protection principles. Bearing the following points in mind will help you to do so:

Personal data shall be processed fairly:

- Publicly available information isn't 'fair game'. Individuals may post their personal details in such a way that they, in effect, become publicly available – for example through a social networking or recruitment site. Wherever you collect personal data from, you still have an overarching duty to handle it fairly and to comply with the rules of data protection. If in doubt, it is good practice, where possible, to contact the person concerned to ask if they agree to their personal data being used in a particular way.

Personal data shall not be excessive:

- Do not collect personal data prematurely. Consider whether you need to collect personal details like names and email address before you allow someone to look at your website. If you cannot justify collecting the information at this point, you should not do so. Asking for too much information too early could also deter individuals from dealing with you.

Once an individual starts to interact with a service provider, for example by asking for details of his or her pension entitlement, or requesting details of a points scheme, it becomes much easier to justify the collection of personal data. Avoid collecting personal data speculatively, on the basis that it may be needed at some point in the future.

- Take care when using an 'off-the-shelf' electronic form, ie one provided by a third party supplier. There is a danger that using the wrong forms could result in the collection of information you don't need, just because a field on the form requires completion. It can annoy individuals when they are asked to provide information for which there is no obvious justification. If you are buying-in 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 specific needs, for example by deleting certain fields or specifying whether their completion is mandatory or optional.

Personal data shall not be kept for longer than is necessary:

- It is good practice to assess periodically whether you need all the information you have been collecting. If you have information that you don't use, you should stop collecting it and should delete any unnecessary information that you have already collected. However, if you are under a legal obligation to keep information for a specific period of time, the DPA will not prevent you from doing so.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data:

- 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.
- Know what personal data you collect and store and who has access to it. Keep an inventory of where the information is stored and keep track of how your organisation collects information eg through email, websites and from other sources. Establish who you are sharing this information with externally and make sure your privacy policy reflects this.
- If your site offers auto-completion facilities for forms and passwords, make sure this will not leave individuals vulnerable, for example if their mobile phone or laptop is stolen.
- 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 are available.
- If you no longer need personal data, make sure you dispose of it securely.
- Assess the risks of a security breach occurring and the potential harm to individuals. Have a plan in place for dealing with security breaches.
- Only allow your staff to access the information they need to do their job. Make sure each user has appropriate access permissions and has 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.

Question 3

Are there any other specific issues relating to online security that you think it would be helpful for us to cover in the code?

Collecting information from 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 disability or do not speak English. There is an overarching duty under data protection law to be fair to the people you collect personal data about, regardless of their level of understanding. It is bad practice to exploit any lack of understanding on the part of the individuals whose information you collect. The law makes it clear that you should not deceive or mislead people. In order to avoid this, you should bear the following points in mind:

- You will not always be able to judge the level of understanding of the people you collect personal data about, although it is likely that a website aimed at children, for example, will be largely visited by them. Therefore you should explain who you are, and why you are collecting information, in a way that the youngest or least experienced people your service is aimed at are likely to understand.
- The more complex the proposition, the less likely it is that a person with a lower level of understanding will understand it. If information is only being collected for a simple purpose such as despatching a free magazine, this may be understood fairly easily by most people. However, it will be more difficult for some to understand the implications of their personal data being used in a more complex way, for example to populate a marketing list for third party use. Because of this, it is good practice to give clear, simple explanations and choices, including opt-outs or opt-ins.
- Given the potential sensitivity of personal data about vulnerable people, including children, it is particularly important to only collect the personal data you need and to keep it secure. If in doubt, do not collect it, or where feasible ask for a parent or guardian's consent before doing so.
- In many cases a parent or guardian should at least be aware of the collection of personal data about their children. However, bear in mind the practical difficulties of obtaining verifiable parental consent.
- You should not encourage vulnerable people to provide personal data about others, eg their friends, by offering prizes or rewards for doing so.

Question 4

Do you think the section on vulnerable people is comprehensive enough?

Are there any other specific issues that you think we should include?

8. Marketing your goods and services online

Electronic marketing and advertising is done in various ways. First party advertisers, such as some online retail companies, market their goods by analysing an individual's purchases or items they have looked at and then displaying content, such as a special offer, for an item their previous behaviour suggests they might be interested in. This process often involves the processing of obvious personal identifiers, such as a name and email address – for example where an individual is logged in to his or her account. In other cases, the marketing takes place through a third party. Typically this will involve the third party placing a particular cookie on a device when an individual visits a website. In cases like this, the third party will 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 obtains may still be indicative of a particular individual's online activity and may still involve categorising an individual according to how he or she is 'scored'.

Although online technology is bringing about a new level of sophistication, there is nothing new about targeting content at particular groups of individuals. For example, direct marketing for up-market magazines has been aimed at those living in certain postcode areas, crime prevention advice at those living in other areas. It is established practice in traditional marketing for customers to be sent details of offers based on goods they have purchased previously – for example book club recommendations. Supermarket loyalty schemes can involve sending customers special offers based on their previous purchases. There is nothing intrinsically unfair or intrusive in using personal data in this way.

When visitors to websites are allocated a 'score' indicative of the sort of person they are likely to be and the sort of interests they are likely to have, their profiles are grouped together with others with the same score and content is then targeted at all those within the same group. Although content is not targeted at particular individuals, the process of analysing a visitor's online activity in order to allocate a 'score' to them, and the score itself, will still be subject to data protection law. This does not stop behavioural advertising or other electronic marketing taking place, but where personal data is being used, these activities have to be carried out in compliance with the DPA.

A website publisher will often use a third party to carry out profiling and targeting on its behalf. Where this is the case, the publisher will retain overall responsibility for the processing of personal data. There can be privacy advantages in this, in that the third party will usually not have access to the more obvious identifiers that a 'first party' site owner may hold in respect of its own customers.

In some cases a group of organisations may work together to deliver content through a single portal. They may each collect and use personal data for their own purposes. In cases like this, each organisation retains its own responsibility for the personal data it handles. Where there is doubt about the responsibilities of the organisations involved, it may be necessary to obtain legal advice in order to clarify this.

Although the Information Commissioner receives relatively few complaints about behavioural advertising or online marketing more generally, there is some public concern about personal data being used to observe and analyse online activity in a way that could be considered intrusive or inappropriate. These fears may arise partly from a misunderstanding of the

technology. That is why it is very much in an organisation's interests to be open about the techniques they use and to make it clear what options people have to opt out. This way, individuals can make an informed choice about whether to use a particular website. 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, for example through behavioural advertising.

Making sure people understand

The processes used to create profiles or allocate a score to an individual may be fairly easy for those involved in the industry to understand. However, the levels of understanding amongst the public may be relatively low. Therefore it is good practice to give individuals a clear and simple explanation as far as it is possible of what happens when they visit your website, how information about their visit is collected and analysed and the result of this – eg being targeted with an advertisement for a particular product. The explanation should be given due prominence and be expressed in terms most visitors to your site could understand. It is also important to ensure that individuals are not being misled as to the degree of anonymity they can enjoy when, for example, accessing a health advice website. If you cannot guarantee absolute anonymity, you should be clear about this.

For more information about explaining what you do to the public see the ICO's [Privacy Notices Code of Practice](#).

'Turning it off'

Many individuals will want to visit a website without any record of their online behaviour being created. Therefore it is good practice to give individuals a simple means of disabling the targeting and profiling process. It is a legal requirement to tell the individual when information is being stored on their equipment, for example in the form of a cookie, and to give them the opportunity to refuse this.

It is good practice to offer individuals relevant advice about how they can use their browser settings, or the choices offered on the website itself, to preserve their online anonymity as far as possible, or to ensure information identifying them is erased at the end of a session.

For more advice about cookies see the ICO's guidance on the [Privacy and Electronic Communications Regulations](#).

Question 5

Have we properly reflected the issues relating to the marketing of goods and services online?

9. Privacy choices

By 'privacy choices' we mean the options that people are given on browsers or websites that allow them to exercise a degree of control over their online personal data. For example, they allow people to choose whether to accept cookies, whether a record of their previous browsing activity (ie 'history') is kept, or whether the information needed to complete a form automatically is retained. These choices also allow users to enable facilities that 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 a person's interests or geographical location.

Default settings

In practice, many individuals may not make use of 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. In addition, they may fail to access or read a company's privacy policy. This is why privacy defaults need to be set in a way that strikes the right balance between privacy protection and functionality. This will help website publishers to comply with their legal obligations, particularly the need to ensure that personal data is processed fairly.

It is good practice for organisations collecting personal data 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 conditions to place on its use. It is good practice to give privacy choices sufficient prominence and to use language that most users are likely to understand.

Despite an organisation's best efforts to make individuals aware of the privacy choices available to them, many will continue to ignore them. It is bad practice for organisations to take advantage of individuals' failure to make appropriate use of the privacy choices available to them. Organisations remain under a duty to collect and use personal data in a way that is fair to the people it is about. Again, this is why the appropriate use of privacy default settings is particularly important.

It is good practice to set privacy defaults to reflect the likely wishes and expectations of the individuals you deal with and the nature of your business. If there is evidence that a substantial number of individuals are altering their privacy settings from the default position, this could mean that the default is set inappropriately and ought to be amended to correspond more closely with individuals' wishes. Where possible, it is good practice to monitor this and to make any necessary adjustments.

Question 6

Should we try to develop specific recommendations relating to default settings? If so, do you have any suggestions on how these defaults could be set? What areas of activity do you think we should cover?

10. Operating internationally

The DPA says that personal data transferred overseas shall enjoy an adequate level of protection. This principle can be difficult to comply with because the nature of the internet is such that organisations operating online will often be operating internationally. For example:

- UK organisations may collect personal data about citizens of other countries.
- Overseas organisations may collect personal data about UK citizens.
- UK organisations may use equipment overseas to carry out their business.
- Overseas organisations may use equipment in the UK to carry out theirs.

The DPA says that organisations established in the UK, or non-European ones using equipment in the UK, must comply with UK law. However, when collecting, storing, using or distributing personal data across international borders, organisations in the UK and elsewhere may have to comply with several different sets of rules. This can raise real practical difficulties, compounded by the fact that developments such as ‘cloud computing’ mean that, in practice, an organisation may not know where information it is responsible for is being processed at a particular time. However, the adoption of good practice will, in many cases, help organisations to comply with the various rules they may be subject to.

Companies established in the UK must try to ensure that all the DPA’s rights and protections are afforded to all the individuals they collect personal data about, regardless of where they are.

Points to remember:

- Use the principles of the UK’s data protection law as the foundation of your compliance, but be prepared to take different, or additional, measures, depending on the people you are collecting personal data about, the nature of the service you are providing and the place or places you are operating from. It is good practice to adopt a ‘highest common denominator’ approach, in order to pre-empt problems and, as far as it is possible, to protect personal data across international borders.
- When collecting personal data from people from a range of countries, it is good practice to try to understand any relevant cultural values and expectations. If in doubt, seek advice from the relevant overseas agencies or consumer protection bodies - particularly where an online service is aimed at a particular group.
- 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 the DPA does not give individuals a right to insist that their personal data is only processed in one country and not another.

Using ‘online’ services

The advent of cloud computing, ‘software as a service’ or ‘distributive computing’ as it is sometimes known, means that organisations increasingly store and process personal data online. The way these services work means that, in practice, an organisation may not know where personal data it is responsible for is located geographically at any particular time. The information may move around the world’s storage facilities according to their current capacity.

The DPA does not prohibit the overseas transfer of personal data, but it does say that it should enjoy adequate protection wherever it is located. Clearly, this raises compliance issues that organisations using cloud computing need to address.

Cloud computing is a fairly recent phenomenon. However, the compliance issues it raises are not substantively different to those that arise when using a contractor in a more traditional context. The key here is to ensure that using a data storage service does not involve relinquishing control of the personal data you have collected, or exposing it to risks that would not have arisen had the data remained under your control in the UK.

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. Modern techniques increasingly allow certain processing operations to be carried out whilst maintaining the security and integrity of the data.

There can be advantages for your company's back-up and security procedures if multiple copies of personal data are held in multiple locations. This can minimise the effect of a serious IT failure on a single site. Nevertheless, it is good practice to conduct a risk analysis prior to contracting with an online services company. This may include the following questions:

If your organisation is thinking of using an online services company:

- can it provide guarantees as to the reliability and training of its staff, wherever they are based? Do they have any form of professional accreditation?
- can it offer an assurance that the data will only be processed in accordance with your instructions – for example that it won't be retained for longer than you wish? Is this in a written contract?
- 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 a standard office software format so that you hold useable copies of vital information at all times?

If answering any of these questions raises serious concerns about a company's ability to look after your information and comply with the law as you would, you should consider using a different firm, or keep services in-house.

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

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

- assure people about your technical security arrangements?
- guarantee that your staff are trained and vetted to suitable standards, wherever they are based?
- guarantee that data will only be processed in accordance with your clients' instructions, eg that it will not be retained for longer than instructed?
- explain your capacity to deal with serious technological or procedural failures?
- explain your complaints and redress procedure eg do you offer compensation for loss or corruption of clients' data?
- explain the facilities you offer to maintain high data protection standards, 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?
- provide your customers with copies of their information regularly, in a standard office software format, so that they hold useable copies of vital information at all times?

If you cannot answer these questions to your potential clients' satisfaction, you may be at a competitive disadvantage. It could be helpful to display any relevant standards that your business complies with, eg security, on your website.

For guidance on the law on data transfers abroad, please see our [legal guidance on international transfers](#). This and other guidance is available on the [international transfers page of our website](#) or on request.

Please also see [The Guide to Data Protection](#).

Question 7

Are there any other international issues you would like to see covered?

11. Individuals' rights online

The law says that organisations that hold personal data must use it fairly and lawfully, keep it secure and make sure it is accurate and up to date. Under the DPA, individuals have certain rights over their personal data; these include the right to see the personal data which you hold about them and to have it corrected if it is wrong. Individuals also have the right to stop their personal data being used for direct marketing. These rights apply to personal data collected online as well as information collected in more traditional ways.

The right of subject access

This is the right that allows people to obtain a copy of information about them. In many cases this will be a straightforward matter, particularly where an organisation keeps obvious identifiers about people, for example in connection with an online healthcare record, bank account or credit reference file. However, the situation can be less clear when only non-obvious identifiers, such as IP addresses, are held.

There will be many cases where an organisation either has no interest in, or no conclusive certainty of, the 'real world' identity of an individual. However, the non-obvious identifiers it holds, e.g. logs of visitors' IP addresses, may allow it to differentiate the activities of one individual from those of another. The records concerned will be personal data in so far as they record a particular individual's online activity, for example the time and duration of his or her website visit. However, there are significant practical difficulties in granting subject access to information of this sort.

There is a major privacy risk inherent in granting subject access to information that is only logged against an IP address or cookie rather than against other information more closely related to a particular individual. The problem arises because the information held is linked to the device used to go online, rather than 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 seek to enforce the right of subject access. However, this is still information that needs to be carefully protected because of the potential 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 to, we would expect subject access to be given. This might be the case where an individual has provided his or her 'real world' personal details in order to register for an online service.

In an online context, it is good practice to use your technology to make it easier and quicker for people to exercise their rights, for example by giving real-time, online access to their personal data. This will not always be possible, for example, where information has to be vetted prior to its release. However, in many cases online facilities can give people an enhanced right of access and can help to keep down administrative costs for organisations.

It is good practice to make it easy for individuals to contact you if they have a problem with their personal data. You should provide the details individuals need to contact you in a prominent place. You could do this by displaying them, or a link to them, on your home page or by including them in your privacy notice. This should be accessible to people at the point you collect their information. You should always make it easy for people to contact you, to change their details or preferences, or to access and correct their information via online facilities wherever possible.

Collective responsibility

It can sometimes 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. A number of different organisations may be responsible for the content that is present on a web page, some of which may involve the processing of personal data. It is good practice for the company with primary responsibility for the website to act as a single point of contact for the content displayed on its site, even if it is not legally responsible for third party content. At least, the company with primary responsibility should help members of the public to contact the third party should they be concerned about their personal data.

Sorting problems out

It is bad practice to require people to contact you by post to resolve a problem with their personal data if it was collected online. It is also bad practice to require people to incur a cost to exercise their rights, for example by only providing a premium rate telephone line to get an inaccuracy corrected. However, the law does allow a fee, generally £10, to be charged for giving people a copy of their personal data.

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, you should meet these requests as soon as possible, unless you have a compelling business need or are under a legal obligation to retain the information. You should always make it clear to people what will happen to their information and tell them whether it will be irretrievably deleted, deactivated or archived. Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it.

It is good practice to monitor customer complaints 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 the expectations of the individuals you deal with. Further information on individuals' rights, and guidance to help you to comply with them, is on the [ICO website](#).

Things to avoid

In conclusion, there are several things that must be avoided by organisations if they are to minimise the risk to the individuals whose personal data they collect. These are:

- Do not be secretive or deceptive in the way you handle people's personal data.
- Do not try to gain an advantage by using personal data in a way that people wouldn't expect or might object to.
- Do not collect personal data you don't need – this involves extra storage costs and additional risk – for example if there is a data loss.
- Do get the best security you can afford – a big data loss or a loss of sensitive personal data could undermine public confidence in your company and cause great commercial damage.
- Do not assume that because you are based in the UK you can ignore other countries' laws. If you use equipment in another country or collect personal data about people outside the UK, you may need to comply with other countries' laws.

Question 8

Does this chapter clearly explain how individuals' rights apply in an online context?

12. General consultation questions

Question 9

Overall, do you think the draft code of practice is useful? If not, what would improve the final code?

Question 10

Did you find the code easy to read and understand?

Question 11

Do you think the advice given in this code meets the realities of current business practice?

Question 12

Are there any key areas that we have not covered?

Question 13

Do you have any comments on how the code should be presented? For example, by a set of web pages with a related discussion forum?

Question 14

We will be providing examples of good and bad practice in the final code. Are there any good or bad practice examples that you would like us to include?

Question 15

Are there any additional features you would like, for example interactive multi-media examples of good and bad practice when processing personal information online?

Question 16

Is there any other relevant guidance that we should refer to? We would welcome suggestions of useful links to other websites that could be included in the code.

Question 17

Are there any further comments you wish to make?

13. How to respond to the consultation

To respond to this consultation please use our online consultation portal. This can be found at <http://ico-consult.limehouse.co.uk>.

Alternatively you can send your response by letter to: Data Protection Development Team, ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

The closing date for responses is: **5 March 2010**.

If you have any questions about this consultation please email us at: consultations@ico.gsi.gov.uk.

Publication of responses

Following the end of the consultation we shall publish a paper summarising the responses.

Information you provide in your response to this consultation, including personal information, may be published or disclosed in accordance with the Freedom of Information Act 2000 (FOIA). If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence.

In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the ICO.

The ICO will process your personal data in accordance with the Data Protection Act 1998 and in the majority of circumstances this will mean that your personal information will not be disclosed to third parties.

Publications Line

t: 08453 091091

f: 01625545808

Helpline

t: 01625 545745

f: 01625545808

e: mail@ico.gsi.gov.uk

w: ico.gov.uk

