Data Protection Act 1998

Compliance advice

Website Frequently asked questions

1 IF WE COLLECT PERSONAL DATA DIRECTLY FROM INDIVIDUALS VIA OUR WEBSITE, WHAT INFORMATION SHOULD WE GIVE THEM?

For the processing of personal data to be fair, website operators who collect personal data directly from individuals must always ensure that individuals are aware of:

- the identity of the person or organisation responsible for operating the website and of anyone else who collects personal data through the site;
- the purposes for which they intend to process the personal data;
- any other information needed to ensure fairness to individuals, taking into account the specific circumstances of the processing. This will include informing individuals of any disclosure of information about them to third parties, including disclosure to companies within the same group.

Unless it is obvious, website operators must give this information to individuals before they collect any personal data from them.

It should be remembered that visitors to a website will not necessarily enter it through its homepage. They may, for example, come directly to a particular page via a hypertext link. The above information should therefore be provided at any point at which personal data are collected.

It should also be borne in mind that there may be more than one data controller involved in the collection of personal data on a website, particularly where banner advertising is placed by a third party, or where a third party provides a secure payment mechanism. In such cases all data controllers should be identified.

Where information is to be used or disclosed for direct marketing purposes, individuals should be provided with the opportunity to prevent this.

Website operators may wish to adopt the Information Commissioner's padlock symbol (*http://wood.ccta.gov.uk/dpr.dpdoc1.nsf*). *This* alerts individuals to the fact that their information is being collected, and draws their attention to the explanation of how it is to be used. Further information about the symbol is available on the Commissioner's website.

2 WE HAVE A PRIVACY STATEMENT ON OUR WEBSITE. IS THIS SUFFICIENT?

Although a privacy statement is important, it is not sufficient to provide the above information simply in the form "click here to view our privacy statement". At least the basic messages and choices should be displayed in an intelligible and prominent form wherever personal data are collected, even where a more detailed explanation is provided elsewhere by means of a privacy statement. Clearly, any basic messages or information given about choices should correspond with the contents of any privacy statement.

Help in designing a privacy statement is available. The Organisation for Economic Cooperation and Development (OECD) has developed a privacy policy generator. This is available at www.oecd.org under 'OECD tools'. As a matter of good practice and as an aid to encouraging confidence, a privacy statement should describe not only what a website operator does with personal data but also what it does not do. It should also tell individuals something about their rights and how to exercise them. For example, individuals have a right to be told whether data about them are being processed and to have a copy of the data. They should be told how to go about this. The privacy statement must include the physical address of the website operator unless this is clearly available on the site.

3 IF WE WANT TO USE PERSONAL DATA OBTAINED VIA OUR WEBSITE FOR DIRECT MARKETING OR TO DISCLOSE PERSONAL DATA TO THIRD PARTIES FOR THEIR DIRECT MARKETING PURPOSES, SHOULD WE PROVIDE AN "OPT-IN" OR AN "OPT-OUT" FACILITY FOR INDIVIDUALS?

The general standard to ensure compliance with the Data Protection Act 1998 is for a website to provide an individual with an opportunity to opt-out of the use or disclosure of their personal data for direct marketing, whether by email or other means. This requires a statement along the following lines:

"We would like to e-mail you with offers relating to products of ours that we think you might be interested in. Click here if you object to receiving such offers."

And/or

"We would like to pass your details on to other businesses so they can e-mail you with offers of goods/services that you might be interested in. Click here if you don't want your details to be passed on."

It should be easy for the individual to register his or her wishes. It would not be acceptable, for example, to expect an individual to visit another site to register his or her wishes, or to register his or her wishes by post.

In some cases an opt-out facility will not be sufficient. This is likely to be the case where the processing of sensitive personal data is involved. Where sensitive data about an individual are collected it will usually be necessary to obtain the data subject's explicit consent to the processing before collecting the information. Sensitive data, as defined in the Act, are information as to a person's:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical or mental health
- sexual life
- commission of criminal offences
- involvement in criminal proceedings

Where explicit consent is required a statement along the following lines will be needed:

"We keep information you have provided us with about your health in order to send you offers of vitamin supplements we think you are likely to be interested in. Click here to show that you agree to this."

It should be noted that explicit consent cannot be obtained by the presence of a pre-crossed box. The individual must take some positive action to signify consent and must be free not to consent.

4 WE HAVE HEARD THAT SOME OTHER COUNTRIES ALWAYS REQUIRE AN OPT-IN TO USE PERSONAL DATA FOR MARKETING. IS THIS TRUE?

Our understanding is that within the European Union the general standard is 'opt-in' in Germany, Denmark, Finland, Sweden and Italy. There are also developments which may lead to an 'opt-in' standard being adopted throughout the EU. For the time being the situation in the UK is that in most cases the opt-in standard is not currently legally enforceable. However, if a website operator wishes to adopt best practice or aspires to market to individuals on the basis of permission or consent, an opt-in is a better indication of a person's wishes than a failure to opt-out.

5 ARE WE ALLOWED TO ASK VISITORS TO OUR WEBSITE FOR INFORMATION THAT WE ONLY WANT TO SUPPORT OUR MARKETING ACTIVITIES?

There is nothing to stop you doing this but you must not mislead your visitors. This is a common problem with websites. If personal information is only required for marketing and is not strictly necessary for the supply of a product or service it should be made clear to visitors why the information is being requested and its supply should be optional. Wording along the following lines might be used, "You do not have to answer the following questions but if you do so your answers will help us understand you better as a customer. We will then be able to bring to your attention offers that we believe you are likely to be interested in".

6 WHAT ARE THE IMPLICATIONS IF WE USE 'COOKIES' TO BUILD UP PROFILES OF VISITORS TO OUR SITE?

Through tracking the on-line movements of an individual, a website operator is able to develop a profile of that individual, which may be used for targeted advertising. If the operator intends to link this profile to a name and postal address or even an e-mail address, there is no doubt that the profile information is personal data subject to the Act. However profiles can be developed and used by means of 'cookies' without the collection of traditional identifiers. The Commissioner takes the view that in the context of the on-line world the information that identifies an individual is that which uniquely locates him or her in that world, by distinguishing him or her from others. Thus profiles that are based on cookies and that are used to deliver targeted marketing messages to particular individuals are personal data.

Cookies are used in a variety of ways by websites. They are not always used to develop profiles of individual site visitors but a visitor must be informed wherever a cookie or other tracking system enables the collection of personal data. This might be done via an

on-line notification that appears before data collection begins, or via the website's privacy statement. However, if a notification provided via an on-line privacy statement is to be relied upon it is important that at least some reference to the use of tracking technology is clearly displayed to all site visitors.

7 Is The Position The Same If We Use IP Addresses To Profile Our Site Visitors?

In theory yes, but in practice it is difficult to use IP addresses to build up personalised profiles. Many IP addresses, particularly those allocated to individuals, are dynamic. Each time a user connects to his or her ISP he or she is allocated an IP address. This IP address will be different each time. Thus it is only the ISP that can link the IP address to an individual. It is hard to see how the collection of dynamic IP addresses without other identifying information would bring a website operator within the scope of the Data Protection Act 1998.

Static IP addresses are different. As with cookies they can be linked to a particular computer which may actually or by assumption be linked to an individual user. If static IP addresses were to form the basis for profiles that are used to deliver targeted marketing messages to particular individuals they, and the profiles, would be personal data subject to the Data Protection Act 1998. However, it is not easy for a website operator to distinguish between dynamic and static IP addresses. Thus the scope for using IP addresses for personalised profiling is limited.

If dynamic or static IP addresses are collected simply to analyse aggregate patterns of website use they are not necessarily personal data. They will only become personal data if the website operator has some means of linking IP addresses to a particular individual, perhaps through other information held or from information that is publicly available on the internet. ISPs will of course be able to make this link but the information they keep will not normally be available to a website operator

8 Are we allowed to use personal data which is available on the Internet for our own purposes?

Website operators should exercise caution when obtaining personal data from a source other than the individual him or herself. It is by no means the case that the processing of personal data obtained via the internet is free from restriction.

Simply because individuals have put their email addresses in the public domain, perhaps by participating in a chat-room, does not mean they can be used for marketing or other purposes. Those who use "spiders" or other scavenging type programmes to harvest email addresses, or other personal data from the Internet, are likely to breach the Act unless the use they are making of the information is consistent with the purpose for which it was first made available. If e-mail marketing lists are used there is a responsibility to ensure that the personal data on the list were obtained fairly in the first place, bearing in mind the intended use of the list. The user of the list must also respect any relevant conditions put on its use by the source.

Individuals may choose to put information about themselves on the internet, for instance by including their CV on their homepage. They should be wary of doing so as the information is clearly open to misuse. Nevertheless, this does not absolve others from their responsibility for ensuring that if they make use of the information they do so fairly with proper regard for the purpose, whether express or implied, for which it was posted on the internet.

9 WE'VE BEEN TOLD WE CAN USE A WEB-BUG TO COLLECT INFORMATION ABOUT VISITORS TO OUR SITE. WHAT IS A WEB-BUG AND CAN ITS USE COMPLY WITH THE DATA PROTECTION ACT 1998?

A web-bug is a graphics file, generally only 1 x 1 pixel in size, that is designed to monitor who is reading a web page or e-mail message. As with the use of a cookie the use of such a device may well result in personal data being processed. The Act does not necessarily prohibit the use of web-bugs or similar software. However, if the web-bug or similar device is invisible to the person whose on-line activities it is monitoring, it is difficult to envisage how the collection of personal data through the use of such a device can be done fairly. Individuals being monitored through the use of a web-bug or similar device should be informed that monitoring is taking place, who the monitoring is being performed by and for what purposes the monitoring is taking place. The Information Commissioner suggests that data controllers who intend to place a web-bug or similar device give the individual a simple means of refusing or disabling the device prior to any personal information being collected through it.

10 IF WE HAVE COLLECTED INFORMATION ABOUT SOMEONE OTHER THAN DIRECTLY FROM THEM, DO WE HAVE TO TELL THEM THAT WE HAVE GOT IT?

Where information is obtained from a third party, for example where one website operator obtains information about an individual from another website operator, there is still a duty to ensure that the subsequent processing of information about the individual is fair, i.e. that the individual is aware of such matters as the identity of the person or organisation that now holds the information and the purposes for which it is to be used.

In some cases it may be possible for operators to inform individuals of the fact that information about them is to be obtained indirectly, and the purposes for which the data are to be used, before the data are obtained. This might be the case where the operator has already had contact with the individual, perhaps when he or she has registered with a website, and has informed him or her that there is an intention to obtain information from other sources. In other cases the source may already have provided a full explanation to the individual on behalf of the third party website operator. This might be the case where two operators routinely exchange information about individuals, and their respective fair processing notices explain this.

Where individuals do not have the information necessary to make the processing of personal data about them fair, operators should provide the necessary information as soon as is practicable. If there is an intention to disclose personal data, the explanation should certainly be provided no later than the time when the information is first disclosed.

The website operator does not have to contact the individual where it would involve "disproportionate effort" to do so. If an operator believes this to be the case it will have to ensure that it can provide the necessary explanation to any individual who asks for it. It must also keep a record of the reasons why it concluded that providing the information would involve disproportionate effort. Website operators should be aware that the ease by which explanations can be provided on-line, for example by the automated sending of an email, means that the circumstances in which they can rely on this exemption are limited. However, the Commissioner would not normally seek to challenge a website operator's compliance with the Act if after obtaining a legitimate e-mail marketing list, the operator provided the necessary explanation with its first marketing approach rather than separately, as long as the first marketing approach came soon after the list was obtained.

11 OUR WEBSITE IS DIRECTED AT CHILDREN? ARE THERE ANY SPECIAL RULES THAT WE HAVE TO FOLLOW?

Websites that collect information from children may have to put more rigorous safeguards in place to ensure the processing of those children's information is fair. Website operators should recognise that children generally have a lower level of understanding than adults and notices explaining the way their data will be used should be appropriate to this level of understanding and should not attempt to exploit any lack of understanding. The consent of a parent or guardian is necessary where a child is asked to provide personal data unless it is reasonable to believe the child clearly understands what is involved and is capable of making an informed decision.

The Act does not lay down a precise age at which a child can act in his/her own right and the Commissioner does not consider it is valid to try and do so. Much depends on the capacity of the child and the complexity of the proposition that is being put to him/her. As a general rule the Commissioner considers the standard adopted by Trust UK (www.trustuk.org.uk) in its accreditation criteria to be a reasonable one. This is that:

> "Personal data must only be collected from children with the explicit and verifiable consent of the child's parent/guardian unless that child is aged 12 years or over, the information collected is restricted to that necessary to enable the child to be sent further but limited on-line communications and it is clear that the child understands what is involved".

The above standard is based on the definition of a child as a person aged 16 years or under.

There are certain practices that, if adopted, are likely to breach the requirements of the Act. These include collecting personal data relating to other people (for example parents) from children and enticing children to divulge personal data with the prospect of a game prize or similar inducement. If personal data collected from children are to be disclosed or transferred to third parties this should not take place without the explicit and verifiable consent of the child's parent/guardian unless it can be demonstrated that the child really appreciates what is going on and the consequences of his or her actions.

Similarly, where a website operator wishes to publish personal data relating to a child on the Internet the verifiable consent of the child's parent/guardian should usually be obtained. Whether it is necessary to seek the parent or guardian's consent to publication, rather than that of the child, will again depend on the circumstances, in particular the age

of the child, and whether or not the data controller can be certain that the child fully understands the implications of making their information available on the Internet.

Where parental consent is required the website operator must have some way of verifying that this has been given. It will not usually be sufficient to simply ask children to confirm that their parents have agreed by means of a mouse click. It will in all likelihood be necessary to revert to postal communication. If parental consent is the required standard but the website operator concludes that the effort in verifying the consent is disproportionate, the proposed marketing activity or other course of action should not be pursued.

12 WE COLLECT PERSONAL INFORMATION THROUGH OUR WEBSITE. DO WE HAVE TO USE AN ENCRYPTION BASED TRANSMISSION SYSTEM?

A website operator is responsible for the security of its processing of personal data. It must adopt appropriate technical and organisational measures to protect the personal data. The processing of personal data includes its obtaining. A website operator is therefore required to obtain personal data in a way that is sufficiently secure. It is hard to see how this can be done without the use of a secure, encryption-based transmission system if the personal data are in any way sensitive or otherwise pose a risk to individuals, for example because they include credit card numbers.

Website operators should be aware that whilst the use of a secure, encryption-based transmission system will protect personal data whilst in transit, there is a potentially greater threat to the security of personal data once the data have been decrypted and they are held in unencrypted form on a website operator's server. Personal data that are in any way sensitive or otherwise pose a risk to individuals should not be held on a website server or, if they are, should be properly secured by encryption or similar techniques.

13 IF WE USE ANOTHER COMPANY TO HOST OUR WEBSITE WHO IS RESPONSIBLE FOR DATA PROTECTION?

Responsibility for compliance with the Data Protection Act 1998 rests with the data controller, that is the person who determines the purposes for which and the manner in which the personal data are or are to be processed. This is likely to be the website operator rather than the host. A data controller does not have to own the equipment on which the processing actually takes place. A website operator that uses a separate processor, i.e. a person who processes personal data on the operator's behalf, must have a written contract with the processor under which the processor is required to act only on instructions from the website operator and to have in place appropriate technical and organisational security measures.

14 CAN WE PUBLISH PERSONAL DATA ON OUR WEBSITE?

The eighth principle of the Act states that personal data shall not be transferred outside the European Economic Area if the country to which the data are transferred does not ensure an adequate level of protection for the individual in each case. Placing personal data on the Internet potentially involves a transfer to any country worldwide. In many countries

the processing of personal data is not protected by legislation so it will not always be possible for website providers to guarantee the protection of personal data placed on their website. However, all the circumstances of such a transfer can be taken into account when assessing the adequacy of protection provided for the data. In some cases the risks arising as a result of a transfer, even in the absence of protective legislation, may be negligible. This may be the case with information that is already in the public domain, for example publication of details of the sporting achievements of well known athletes. It may also be a relevant factor if the information published does not enable the individual to be contacted, although the sensitivity of the information will have to be taken into account. In other cases it will be necessary to obtain the individual's consent for their data to be published on the Internet. This consent must be 'informed', in that the website operator must explain the possible consequences of publishing the data. Consent must also be 'freely given' in that the individual must be able to decline without penalty.

Although likely to lead to similar conclusions, in most cases the general requirement of fairness in the processing of personal data must also be addressed when considering publication on a website. For example, a yacht club may have traditionally published the names and contact details of its members in a handbook distributed to all members and placed in local libraries. The club now intends to publish these details on its website. Although the information has always been publicly available, the implications for members of publication on the web are significantly different. Fairness requires that the individuals concerned are told that there is an intention to publish information about them on the website and that the wishes of individuals who object are respected. If the intention is that information about the club's membership is only made available to other club members, the club should employ technical means to prevent access by unauthorised individuals, for example, by preventing general access to the site or to the part of the site where information about the club's members is published through the use of password protection.

15 IF WE WANT TO USE THE PERSONAL DATA WE HAVE OBTAINED THROUGH OUR WEBSITE DIFFERENTLY CAN WE SIMPLY CHANGE OUR PRIVACY STATEMENT?

The simple answer is no. Changing the privacy statement and other information on the site can only affect how you can use personal data that are obtained after the date of the change. Visitors who provided you with personal data prior to the change will have done so on the basis of the privacy statement and other information you provided at that time. You must honour the assurances you gave them.

If you want to use the personal data differently the safest course of action is to obtain your customers' consent to the new use. In other words you must explain the proposed new use to them and only proceed when they have given you a positive indication of their agreement. Failure to respond to an e-mail message would not be sufficient. This is sometimes referred to as 'opt-in'. The opt-in approach will be necessary if the data you have obtained are to be used by you or others for a new purpose or are to be disclosed either for the first time or to different organisations from those referred to in your privacy statement. It will also be necessary if the personal data are sensitive or if they are subject to a duty of confidentiality which would be breached by the new use.

In some cases it will be sufficient to advise your customers of the new use and to give them an opportunity to object. This will be the case if the new use does not amount to

use for a new purpose or where the nature and purpose of a new disclosure remains close to the terms described in the privacy statement. For example, your site was originally set up to sell books, your customers were advised only that you would use their information for marketing and they were given an opportunity to opt-out. In the absence of any indication to the contrary they would have assumed your marketing was confined to books. You are now expanding into the sale of CDs and want to market these. As this activity is close to but nevertheless outside the terms of your original privacy statement, you should at least advise those customers that did not opt-out originally of the new use and give them another opportunity to opt-out, either from all marketing or from the marketing of CDs. Those customers that opted out originally should not be contacted.

If in the above example the new marketing is of financial services or holidays, for example, or if customer details are to be provided to a third party for their marketing, the standard has to be opt-in. This will certainly be the case if, for the first time and with no previous explanation the marketing is to be based on a profile of the individual's book buying habits.

In other cases the new use might fall within the original privacy statement. For example, the privacy statement might have referred to the intention to market a range of products even though at the time this was confined to books. Now it will include CDs. There is no need to advise customers specifically of this as the products are sufficiently closely related. Clearly the wishes of any customers that subsequently object to the receipt of the new marketing message should be respected.

If the new products are substantially different, for example if they now include financial services, the marketing of these would not have been within customers' expectations even though arguably the privacy statement might have covered it. It is the interpretation customers are likely to have placed on the privacy statement rather than its precise wording that is important. Depending on how far removed from this likely interpretation the new use is, the standard may be opt-in rather than opt-out.

16 CAN WE DISCLOSE PERSONAL DATA IF OUR WEB-BASED COMPANY IS SUBJECT TO A TAKE-OVER OR MERGER?

The Act would not necessarily prevent this. Essentially the position on disclosure is no different simply because a web-based company goes out of business or is otherwise subject to a take-over or merger. A disclosure could breach the Act where individuals have previously been assured that personal data about them will not be disclosed, where the personal data are subject to a duty of confidentiality or where once disclosed the personal data are processed in a manner that has a markedly different effect on individuals. In such cases the consent of individuals will be required before the disclosure takes place.

Before making a disclosure of personal data careful consideration should be given as to how the data were originally obtained. If a disclosure is to take place, in order to prevent unfairness to individuals it may be necessary to place restrictions on the purposes for which and the manner in which the data may be processed.

So long as individuals were not led to believe their data would never be disclosed, the new owner in effect takes over the existing business and the personal data will be used in substantially the same way as previously. The Act is likely to be satisfied if individuals are

told of the change of ownership and have an opportunity to object to the new owner holding their details.

17 DO WE HAVE TO NOTIFY THE COMMISSIONER IF WE PUT PERSONAL DATA ON OUR WEBSITE OR OBTAIN PERSONAL DATA THROUGH IT?

Website operators who are established in the UK and who process personal data will need to notify the Commissioner unless exempt. Failure to notify is a criminal offence for those required to do so. There are conditional exemptions from notification where personal data are only processed for certain core business purposes. These include advertising and marketing your own business and keeping accounts and records. The exemptions will not necessarily be lost because personal data are obtained through a website or used for marketing by electronic means. They are more likely to be lost through publishing personal data on a website.

Many website operators will need to notify under the Act. You should visit www.dpr.gov.uk for more information about this and to notify. The current fee for notification is £35 for one year.

18 DOES THE DATA PROTECTION ACT 1998 APPLY IF OUR WEBSITE IS OPERATED OUTSIDE THE UK?

Website operators not established in the UK but established elsewhere within the European Economic Area (EEA) will be subject to the data protection laws of the countries where they are established. In some circumstances website operators established outside the EEA might be subject to UK data protection law. If a website operator established outside the EEA uses equipment in the United Kingdom to process personal data, the processing will be subject to the Act even though the operator is not established in the UK. This might be the case where the operator's site is hosted in the UK or where the operator places a 'cookie' on the computer of a UK internet user in order to create a profile of that individual's on-line behaviour.

19. WHAT IS THE POSITION IF I ONLY USE MY WEBSITE FOR DOMESTIC PURPOSES?

Where personal data are processed only for an individual's personal, family or household affairs, including recreational purposes, the data are exempt from the Act's notification requirements and from the requirements of the data protection principles. However, the Information Commissioner retains her powers of investigation and enforcement to determine whether the scope of the exemption has been exceeded, for example because the site is also used for business purposes.

20. IS THIS THE COMMISSIONER'S FINAL WORD ON THE QUESTION OF DATA PROTECTION AND WEBSITES.

No, these frequently asked questions may be updated in the light of technological, legal or other developments. Please let us know if there are questions of general interest to website operators that we have failed to address.

Information Commissioner
Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF Telephone:01625 545 700 Facsimile: 01625 524510
e-mail: data@dataprotection.gov.uk Website: www.dataprotection.gov.uk