

## WING TIPS

### *ICO Guidance on Collecting Personal Information on Websites*

Last year, The Information Commissioner's Office (ICO) published a 'Good Practice Note' on the collection of personal information using websites<sup>1</sup>. This provides some practical guidance which will be relevant to any business that collects or processes personal data via its website.

#### **What information should website operators give to individuals who submit their personal data to a website?**

In the context of a website the Data Protection Act 1998 (DPA) requirement of fair processing means that the website operator must supply fair processing information at any point on the website at which personal data is collected from users. The fair processing information will usually be given in a privacy statement or policy.

Such information should include details of who is collecting the data, for what purpose, how the data will be used and any other relevant information required to make the processing fair in the circumstances, such as whether the information will be disclosed to third parties and in what circumstances. Website users should also be told what their rights are in relation to their data and how to exercise them.

If more than one organisation collects personal information through the website, for example if a third party provides a secure payment system, then each organisation that collects the data should be identified and their use of the data explained.

Active steps must be taken to bring the fair processing information to the attention of the website user. The ICO's view is that simply providing a link to a privacy statement is not sufficient. Instead, wherever personal data is collected on the site there should be some basic description of how the data will be used, with a link from this to the full privacy policy which contains the detailed fair processing information. This accords with the ICO's view that a 'layered' privacy policy is the most effective way of communicating the information. The ICO refers data processors to the Organisation for Economic Co-operation and Development (OECD) website's privacy policy generator<sup>2</sup> which can help to generate a basic tailored privacy statement based on the answers from a questionnaire.

### **Scope of use of personal data**

Website operators may only process personal data for the purposes for which it was originally collected, as set out in the privacy policy that was in force when the website user provided the data. Unilaterally changing the terms of the privacy policy does not give the website operator the right to use personal data for new purposes outside the scope of those envisaged in the previous policy.

The ICO states that the “safest” way for a website operator to change the scope of permitted processing or use of personal data is to gain the express consent of the website user by means of an express “opt-in” route. This will be necessary when sensitive personal data, or data that is subject to a duty of confidentiality, is processed or when the website operator wishes to transfer the data to an organisation other than those listed in the privacy policy.

If the use of the data is not a new purpose, or is sufficiently close to the scope of the purposes or uses set out in the privacy policy that the website user would have an expectation that it would be used in this way then the advance opt-in route will not be necessary. Instead the ICO states that the individual should be informed of the new use and should be given the chance to object to the processing through an “opt-out” route.

### **Using other website tools to collect personal information**

Using cookies or web-bugs (also known as web-beacons) to track a website user’s on-line movements in order to create a profile of the user is not in itself considered to be the collection of personal data. However, if the website operator takes the profile that has been generated by the information collected by the cookies and links it to a user’s name, address or other unique identifying information then the profile itself becomes personal data for the purposes of the DPA.<sup>3</sup>

IP addresses may also be personal data if the website user links the address to other identifying information to create a profile of a website user. However, this will only be possible if the IP address used is static - ie if a specific user is always allocated the same IP address by their internet service provider (most consumer ISPs offer dynamic IP addresses by default).

### **Using personal information found on the web**

Sometimes personal data regarding individuals is made available on the web, either by the individual themselves or by another organisation. The fact that such information is available does not give anyone, including website operators a blanket right to collect and use it for their own purposes; they must still observe the DPA regime and process the data fairly. The ICO considers that it is likely that processing of data collected on the internet in this way will only be “fair” if the data is used for the purposes that it was originally provided for.

It will be up to the website operator to establish whether the purposes for which it intends to use such data are within the scope of those for which the data was published. If not then it may be necessary (depending on the context) to inform the individual of the fact that their data has been collected and of the purposes for which it will be processed. Where the individual has already been informed, at the point at which the data was collected, of this potential use then there will be no need to contact them in this manner.

If contacting the individual would involve “disproportionate effort” then the website operator is not required to do so. However, the decision making process leading to this conclusion should be clearly documented so that the website operator can justify the decision to the ICO, if required to do so. The ICO has noted that now that information can be so easily sent via automated emails there will be limited circumstances in which it will be justified not to contact the individual.

### **Personal data regarding children**

Strong safeguards are required where websites are directed at or used by children. The explanations of why information is being collected from the child should be appropriately worded according to the age group and likely understanding of the child. Parents or guardians should give consent for the collection of personal data

from their child, unless it is reasonable to assume that the child has a clear understanding of what is involved and is capable of making the decision to supply the information on their own. Children should never be asked to give personal data about anyone else or to supply their data in return for the chance to win a prize.

The express and verifiable consent of the child's parent or guardian will be needed to publish a child's information on the internet or to transfer or disclose such information to a third party unless it is clear in the circumstances that the child fully understands the implications of their information being published and has sufficient maturity and understanding to give their consent.

### **Security systems for the protection of personal data**

A website operator must ensure that personal data it processes is protected by adequate and appropriate technical and organisational measures. The ICO's view is that it is difficult to see how this level of protection for sensitive personal and financial data can be achieved unless a secure encryption based transmission system is used. More caution should be exercised where sensitive personal information is stored on a website server and such server must be encrypted.

### **Publishing personal data on a website**

When personal data is published on a website available outside as well as inside the UK the website operator should consider whether this is fair to the individual, in the circumstances. This will involve a consideration of the risks to the individual of having their data made available in this way. It may be that, on balance, fairness will require that the website operator contacts the individual to explain the potential consequences of his data being published on the website, and to obtain his consent.

**To find out more, contact Andy Moseby, Partner, [andy.moseby@kemplittle.com](mailto:andy.moseby@kemplittle.com) or Hannah Sutcliffe, Commercial Technology Assistant, [Hannah.sutcliffe@kemplittle.com](mailto:Hannah.sutcliffe@kemplittle.com) at Kemp Little LLP**

### **Notes**

1 <http://tinyurl.com/yvg98p>

2 <http://tinyurl.com/2drxza>

3 It should be noted that regardless of whether the information collected using cookies or other tracking devices is personal data, Regulation 6 of the Privacy and Electronic Communication Regulations 2003 requires websites to inform website users when the website collects information about them. The site visitor must have the opportunity to refuse the continued use of the tracking device.