Data protection / FoI

Private eye

Tom Morrison kicks off his quarterly review of the world of information law

Photo: © gettyimages.co.uk

IN BRIEF

- Named public authorities have been placed on a "watch list" and are having their FoI compliance monitored.
- A new law regulating the use of website cookies comes into force on 26 May 2011 and will require many websites to be updated.

We are all interested in what happens to our own information—how it is used, to whom it is given and how it is kept secure—and we want to know more about how well public authorities are being run. Former Prime Minister Tony Blair may regret it now, but when he came good on New Labour's manifesto commitment to put the Freedom of Information Act on the statute books he set in train a series of events that would change the expectations of ordinary Joe Public forever. There is no turning back: data protection and freedom of information are here to stay. It will never be a vote-winner for any mainstream political party to pledge to reduce the protection afforded to individuals' personal information, nor will it be popular to campaign on a promise to remove the rights of citizens to access information about how money is being spent in their name.

The regulatory noose has been tightening for some time to the extent that those that flout the Data Protection Act now face genuinely significant fines and serious damage to reputation. Public authorities face the wrath of the Information Commissioner's Office (ICO) if they do not comply with the Freedom of Information Act—and quite possibly the wrath of the media if they do comply and as a result have to disclose embarrassing information. With that in mind this quarterly column has been introduced to provide updates on relevant developments in information law, pointing out significant changes in the legislative landscape, providing tips on how to go about managing obligations, and drawing attention to instances where organisations have got it wrong and had to deal with the consequences.

Freedom of information

Freedom of information hogged the information law limelight for a good while after its full implementation in 2005. The ICO had to continue to grapple with its data protection enforcement obligations whilst tooling up for this whole new area of responsibility. Public authorities' freedom of information officers have started to get to grips with what the disclosure obligations mean for their employers and the case law is starting to make clearer what can legitimately be withheld from the public. We will look at specific examples in future editions, but for the time being it is fair to say that the starting point is that public authorities have a general duty to disclose information if requested, regardless of who has asked for it or what the purpose of the request is. Exemptions to disclosure have to be applied judiciously such that public authorities often find themselves caught between the rock of the party demanding information and the hard place of a third party not wanting the public authority to release sensitive information.

> "You would be forgiven for thinking that data protection is all about data security"

The ICO is starting to increase pressure on those public authorities who, despite having had several years' practice, are still slow in responding to requests. A "watch list" was created, consisting of authorities which the ICO felt needed to be closely monitored over a three-month period. The worst performing have been named and an update on their progress was issued in mid-April. Certain authorities seem likely to suffer regulatory action soon. An updated list has been compiled and a further progress update will be published in the autumn.

Data protection

You would be forgiven for thinking that data protection is all about data security. There are in fact eight principles with which all organisations handling personal information need to comply. Keeping information secure is the seventh. A survey commissioned by the ICO earlier this year found that 96% of those surveyed are concerned that organisations do not keep their personal information secure. Judging by recent enforcement activity their concerns may be well-founded.

The ICO has been issuing press releases with alarming regularity explaining which is the latest company, charity or public sector body to have lost information, how it happened, what action has been taken by the ICO and what the organisation is going to do to put things right for the future. Chief executives are usually required to sign undertakings which are made public; you cannot help but feel sorry for the poor data

protection officer (who is also often the HR or IT manager) who has had to tell the boss that a public flogging is imminent, but it is proving to be an effective way of making sure that data protection stays high on the corporate agenda.

It would perhaps be unfair to list the organisations here, although in future editions we will get into some specific breaches that have taken place in order to elicit the lessons to be learned. The breaches are often ones which could happen within any organisation if adequate procedures are not in place (see box below).

Some serious fines have been issued since the ICO got the power to issue them last year. The smallest so far has been for £1,000, the largest for £100,000. The smallest fine was lined up to be the largest (at £200,000) but the data controller had since gone out of business so rather than risking making the former owner bankrupt the ICO fined him the smaller amount. The maximum fine that the ICO can issue is £500,000, and it can do so without having to go to court. A review of the circumstances leading to the fines will appear in future editions of this column.

And finally...cookies anybody?

The Department for Culture, Media and Sport has recently released a report on the implementation of the revised EU electronic communications framework. One of the more wide-reaching changes concerns cookies, which store information about internet activity on a user's computer having been placed there as a result of visiting a website.

Cookies are commonplace and are often essential to the smooth running of websites which operate shopping carts. Their use has developed over recent years such that tracking cookies (which can determine which websites a user has visited) or cookies which help tailor advertising content based on the user's behaviour are becoming widespread.

This has raised privacy concerns such that from 26 May 2011 the law will require website operators to obtain actual user consent to the use of many types of cookies. Cookies that are "strictly necessary" for a user-requested service (such as those necessary to operate shopping carts) are excluded, but for all other cookies website operators will no longer be able to rely on placing clarification statements in their privacy policies with details of how to opt out.

The necessary legislative changes will be made by amending the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (PECR), although the Government has decided that the practical solutions for how to achieve compliance should originate from industry. If this sounds a little woolly it is for a good reason—it is woolly. The Government has decided that it is not going to attempt to clarify the requirements in the legislation itself, for fear of placing on British businesses obligations which are greater than those placed on their European competitors by their own domestic legislation. Instead our law will be as vague as the other Europeans' law. Initial guidance has just been issued by the ICO, but the Government has stated that it does not wish the law to be enforced in full by the ICO straight away. At the same time it has been made clear that all businesses operating websites which utilise cookies will need to be seen to be actively planning for making changes to their websites in the short term. In particular, any organisation with a website should:

(i) check what type of cookies and similar technologies it uses and how it uses them;
(ii) assess how intrusive that use of cookies is; and
(iii) decide what solutions to obtain consent will be best in the circumstances.

The ICO offers some initial thoughts on potential solutions, but in practice all seem cumbersome. It is hoped that more elegant solutions will emerge in the coming weeks and months. One proposal gathering support is that made by the Internet Advertising Bureau (IAB) for a self-regulatory system, which has suggested that any advertising affected by a user's online behaviour should contain, or be placed near, an icon which shows adherence to the IAB's system. Users can click on the icon and see who is collecting information, what is being collected and why, and will also be able to choose whether their data is collected. If an organisation wishes to harvest data from all or substantially all web pages visited by a computer, it must first obtain explicit consent.

> **"If this sounds a little woolly it is for a good reason...it is woolly"**

In addition to the changes relating to cookies, there have been some substantive revisions that are particularly relevant to providers of electronic communications services. There will be a duty on providers to notify personal data breaches to the ICO. In some circumstances, the person whose data is breached must also be notified by the provider. This is a significant step towards a controversial full-scale data breach law which already exists in other countries, including the USA, but not yet in Britain.

The ICO has also obtained stronger enforcement powers in relation to PECR. Telephone and internet service providers may be made subject to third party information notices which enable the ICO to track companies who cold call or send spam whilst masking their identities. Those organisations which conduct unsolicited e-mail or telephone marketing may also be fined up to £500,000.

More to come

The past few years have seen an unprecedented degree of change in the laws regulating both the use of personal information and the disclosure of public information. The enforcement mechanisms have been bolstered and the body of case law is maturing. No business, charity or public sector organisation will want to be the subject of an ICO press release, so the need to keep up to speed on this evolving body of law has never been greater. NLJ

Tom Morrison is a partner at Rollits LLP. E-mail: *tom.morrison@rollits.com*. Website: *www.rollits.com*

Data breaches: common threads

- The use of memory sticks, laptops and other portable devices should be restricted and all should be encrypted.
- Password protection on its own is not enough to demonstrate that adequate security measures have been put in place.
- Staff need to be well-trained in taking care that faxes and e-mails are sent only to the intended recipients.