Adams & Remers

A&R Legal Briefing

Digital Commerce: a round up of recent news and views

Opt in, Opt out, shake it all about

As reported in our previous article on cookies - Have your cookie and eat it: guide to website cookies rules changes, the E-Privacy Directive changed the requirements that online providers must meet when using cookies from the opt-out regime that was previously in force, to a requirement for informed consent.

In May 2011, the Information Commissioner's Office ("ICO") published its guidance on the changes, but was unclear as to how the issue of consent should be dealt with. In December 2011, the ICO published updated guidance and was of the view that user awareness was not good enough for websites to rely on as implied consent to the use of cookies. It continued to advocate an opt-in regime.

The ICO's latest guidance (issued in May 2012) acknowledges that an explicit opt-in mechanism might provide regulatory certainty but confirms that in some circumstances implied consent might be a valid and more practical option. Implied consent can only be relied upon however, if it is specific and informed, and there is some action on the user's part from which consent can be inferred. If a website includes a clear and unavoidable notice that cookies will be used if the user enters the site, and the user clicks through and continues to use the site on that basis, this will be sufficient to imply consent.

The ICO's u-turn on the issue of implied consent will be good news for UK website operators. It means we are back to an opt-out regime. For the time being, at least.

Is your head in the clouds?

More and more businesses are looking to use cloud computing, with the economies of scale they offer giving access to a range of computer technologies and expertise that would be difficult to afford in-house. But by processing data in the cloud, businesses may encounter risks to data protection that they were previously unaware of.

Data controllers must take the time to understand these risks: they remain responsible for how personal data is looked after, even if they pass it to cloud network providers. The ICO has recently published guidance to help businesses navigate their data protection obligations in the clouds. The guidance gives tips including:

- Be selective: select the right cloud service and cloud provider and select which data to move to the cloud (it may not be necessary to move it all);

- Be risk aware: seek assurance on how the data will be kept safe both in the cloud network and physically, in a data centre;

- Be compliant with legislation: the law requires a data controller (i.e. the business itself) to have a written contract in place with all outside organisations that process its data, including those providing cloud services;

- Be transparent: the cloud provider must not process the cloud user's personal data without his agreement. This means that the business itself must ensure that appropriate consents have been obtained from the user at the point of collection of his data, to the processing of his data in the cloud;

- Be location sensitive: don't forget that transferring data internationally brings additional obligations – that includes using cloud providers whose servers are located abroad.

The ICO's view is clear: "*as a business, you are responsible for keeping your data safe. You can outsource some of the processing of that data, as happens with cloud computing, but how that data is used and protected remains your responsibility*".

Data Protection: a compliance reminder

We are all aware of the horror stories in the press regarding the careless loss or disclosure of personal data by Government entities, the police and even charities. But it is worth remembering that no business organisation is immune from investigation by the ICO for breaches of the Data Protection Act 1998.

In November, Prudential was fined £50,000 following a mix-up over the administration of two customers' accounts, which led to tens of thousands of pounds meant for an individual's retirement fund, ending up in the wrong account. The original error was caused when the records of both customers, who share the same first name, surname and data of birth, were mistakenly merged in March 2007. The accounts remained confused for more than three years, and the problem was only resolved in September 2010. This was despite Prudential being alerted to the mistake on several occasions, including in late April 2010 when one of the customers notified it that his address had not changed for over 15 years. The company failed to investigate thoroughly at this point, and the penalty imposed by the ICO relates to the inaccuracy in the data then present, which continued for a further 6 months.

This is the first monetary penalty served by the ICO which does not relate to a significant data loss. The ICO's view was that organisations must make sure that the information they hold on their customer files is accurate and kept up to date. The Prudential's failure to do so (and its failure to remedy the situation despite having been notified of the problem on more than one occasion) was deemed by the ICO to be a serious breach of the Data Protection Act 1998.

According to the ICO: "while data losses may make the headlines, most people will contact our office about inaccuracies and other issues relating to the misuse of their information…we hope that this penalty sends a message to all organisations…that adequate checks must be in place to ensure people's records are accurate.

Perhaps a brief reminder to all is needed: anyone who processes personal data must ensure that it is:

- processed fairly and lawfully
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept longer than is necessary
- processed in line with an individual's rights
- secure
- not transferred to other countries without adequate protection

Jingle bells, online sales

The OFT recently conducted a pre-Christmas review of 156 retailer websites and found that many of them may not be complying fully with the Consumer Protection (Distance Selling) Regulations 2000 and the Electronic Commerce (EC Directive) Regulations 2002.

These regulations cover the sale of goods and services online or via digital television, by mail order (including catalogue shopping, telephone or fax). They give consumers the right to receive information at certain stages of the ordering process, and certain rights regarding delivery, performance and cancellation. The regulations are compulsory and retailers cannot exclude them.

Key failures highlighted by the OFT included:

- imposing unreasonable restrictions on customers' rights to a refund: the most common restriction was to require the customer to return the product in its original packaging or condition, which the OFT noted could infringe on consumers' rights to reasonably inspect or assess the product;
- failing to provide an email contact address: a web contact form is insufficient; and
- indicating up front that compulsory charges are to be added to the price shown, but then adding further unexpected charges at the checkout stage.

The OFT's review is part of its ongoing work to ensure that consumers are able to shop confidently online. It has indicated that retailers not complying with the law will face enforcement action by the OFT or local Trading Standards. These bodies have the power to consider complaints and seek court orders for compliance, which does not bode well for retailers from a customer satisfaction perspective.

In the spirit of festive cheer and goodwill to all men, perhaps now is the time for businesses that sell goods to consumers over the internet to review their online terms and conditions to ensure that they comply with all consumer protection law.

If you would like assistance, please contact Aisha Dickson

Aisha Dickson

Contact

Aisha Dickson
Associate

Tel **+44(0)1273 403265**

Email
aisha.dickson@adamsandremers.com

Further Help & Advice

Lewes

Trinity House, School Hill,
Lewes, Sussex, BN7 2NN

Tel +44 (0)1273 480616
Fax +44 (0)1273 480618
DX 3100 Lewes1
Email **lewes@adamsandremers.com**

London

Commonwealth House,
55-58 Pall Mall, London, SW1Y 5JH

Tel +44 (0)20 7024 3600
Fax +44 (0)20 7839 5244
DX 140545 Piccadilly 5
Email **london@adamsandremers.com**