RegulatoryStrategies

UK Data Protection Newsletter March 2013

Headlines this month:

- Changes to ICO website and email address
- Open letter from the ICO and OFCOM to marketing companies
- Lack of guidance from employers on use of personal devices
- CCTV Guidance
- Commons Justice Select Committee report
- EU Commissioner - new framework is not just about consent
- Recent data breaches

Commentary:

Changes to ICO website and email address

The ICO has changed its website and email address from ico.gov.uk to ico.org.uk to reflect its independence from government.

Open letter from the ICO and OFCOM to marketing companies

The ICO is working with OFCOM, who hold responsibility for regulating silent calls, and will be sending an open letter to marketing companies. The letter will remind companies of their legal and regulatory obligations and that the failure to meet these will be result in enforcement action. The ICO can fine up to £500,000 for serious breaches of the Privacy and Electronic Communications Regulations. OFCOM can fine up to £2,000,000 for breaches of rules associated with abandoned and silent calls.

The ICO continues to headline its reporting tool on its website to encourage members of the public to report details of unwanted marketing texts and calls. A recent fine relating to a breach of PECR and further proposed enforcement action is outlined later in this Newsletter.

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

Lack of guidance from employers on use of personal devices

A recent ICO commissioned survey has shown that many organisations too often allow staff to use personal laptops or smartphones for business purposes potentially placing personal information at risk.

The survey was carried out for YouGov and showed that 47% of adults use their personal equipment for business purposes but less that 3 out of 10 are provided with guidance about how devices should be used. The results of the survey coincide with guidance issued by the ICO highlighting risks of using personal devices to process personal information and the fact that a Data Controller will have significantly less control of the information.

Organisations should be assessing:

- The type of data being held
- Where data may be stored or transferred
- The potential for data loss
- Possible blurring of personal and business use
- The security of devices
- Procedures for when an individual leaves the business
- How to manage loss, theft, failure and support of a device

CCTV Guidance

The ICO has issued guidance for organisations and the general public about when CCTV use is covered by the Data Protection Act. The guidance for organisations is comprehensive and detailed helps to determine when and how CCTV should be used and how it should be administered.

The guidance makes clear to the public that most uses of CCTV are covered by the Act which consequently gives individuals the right to see what information is held about them outlining the few exceptions to this rule eg cameras for household purposes.

The guidance makes clear that:

- CCTV operators must make clear that individuals know that CCTV is being used. Signage must be clear and visible and show the name of the organisation operating the system
- CCTV should only be used in exceptional circumstances when privacy would normally be expected eg changing rooms or toilets. Extra efforts should then be made to make clear that cameras are being used
- Conversations between members of the public should not be recorded other than in a few specific exceptions
- The CCTV operator should ensure someone in the organisation has responsibility for CCTV images
- Notify the Information Commissioner's Office
- Have procedures about system use
- Regularly monitor that procedures are being followed

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

The guidance reinforces that individuals have subject access rights to obtain CCTV images that relate to them. As with all subject access responses, the organisation can charge £10 and must send a response within 40 calendar days. The guidance goes on to explain:

- Operators cannot provide images of identifiable people to the media or post them to the internet for entertainment
- An organisation may need to use images for legal purposes
- Images should be subject to a retention policy and only retained for as long as necessary

Commons Justice Select Committee report

The Justice Select Committee has issued its report on 'The functions, powers and resources of the Information Commissioner". The report was based upon evidence given in February. The report raises concerns about the funding of the Information Commissioner's Office in view of the proposed new EU data protection legislation and the recommendations made by the Leveson Inquiry. The report quotes a potential shortfall of funding of £42.8 million.

Some of the conclusions and recommendations of the report include:

- If Government require the ICO to expand its role in monitoring data protection in the press, in light of the Leveson Inquiry, it should have the resources to do so
- The Information Commissioner will need to keep Government informed about developments in the proposed data protection reforms to ensure that the implications are appreciated and resource will be sufficient to meet these
- It is recommended that the Information Commissioner should become directly responsible to, and funded by, Parliament
- Consideration should be given by Ministers regarding making breaches of Section 55 of the Data Protection Act recordable offences
- Public sector organisations should, as a general rule, accept the offer of a free audit from the Information Commissioner
- The Secretary of State should bring forward and order under Section 41A of the Data Protection Act to meet the recommendation of the Information Commissioner that his power to serve Assessment Notices can be extended to NHS Trusts and local councils

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

EU Commissioner - new framework is not just about consent

The EU Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, has stated that explicit consent is a key factor in the proposed data protection reform but it is nothing new.

Reding states:

"The current Directive states since 1995 that consent has to be 'unambiguous'. The Commission thinks it should be 'explicit'. 27 national Data Protection Authorities agree. This has become a major talking point. What will this mean in practice? That explicit consent will be needed in all circumstances? Hundreds of pop-ups on your screens? Smartphones thrown on the floor in frustration? No. It means none of these things. This is only the scaremongering of certain lobbyists."

Reding has stated that consent needs to be explicit because citizens do not understand the notion of implicit consent:

"Legitimate interest is the ground that is currently used by the marketing industry for example. It will continue to be used by the marketing industry. From the perspective of this Regulation, consent is irrelevant in such cases. It will continue to be irrelevant."

Reding added that explicit consent is needed when processing becomes more intrusive.

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

Recent data protection breaches

DM Design

TDEM Design, a Glasgow based firm, has been fined £90,000 by the Information Commissioner's Office further to almost 2000 complaints to the ICO and the Telephone Preference Service.

The fine was the result of the company failing to check whether individuals had opted out of marketing calls. In one instance an employee refused to remove a complainant's details from the company's system and threatened to "continue to call at more inconvenient times like Sunday lunchtime".

This fine is the first that the ICO has issued for a serious breach of the Privacy and Electronic Communications Regulations relating to live marketing calls. However, a fine of £440,000 was issued to a company responsible for sending thousands of spam texts in November 2012.

Two other companies have been informed that the ICO is intending impose significant penalties and a further 10 companies are undergoing investigation for cold-calling and sending spam messages.

Christopher Graham, the Information Commissioner, commented:

"Today's action sends out a clear message to the marketing industry that this menace will not be tolerated. This company showed a clear disregard for the law and a lamentable attitude toward the people whose day they were disturbing...

..This fine will not be an isolated penalty. We know other companies are showing a similar disregard for the law and we've every intention of taking further enforcement action against companies that continue to bombard people with unlawful marketing texts and calls."

Doctor's receptionist

A for receptionist in a GP's surgery has been prosecuted by the Information Commissioner's Office for unlawfully accessing sensitive information about her ex-husband's wife. The receptionist was prosecuted under Section 55 of the Data Protection Act, fined £750 and charged a £15 victim surcharge and £400 prosecution costs.

David Smith, the Deputy Commissioner and Director of Data Protection, commented:

"This case clearly shows the distress that can be caused when an individual uses a position of responsibility to illegally access sensitive personal information."

Offences under Section 55 of the Act can be punishable by fines up to £5,000 in a Magistrates Court or unlimited fines in Crown Court. The ICO used the opportunity to urge the government to proceed with tougher penalties for offenders.

Visit our website at www.regulatorystrategies.co.uk

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk