RegulatoryStrategies

UK Data Protection Newsletter October 2012

Headlines this month:

- The evolving data protection landscape - 2012 and beyond
- Information Commissioner's Office states that private sector leads the way on data protection compliance
- Organisations warned to encrypt data
- ICO's view on the draft Communications Data Bill
- Definition of personal data
- Recent data breaches
- EU update

Commentary:

The evolving data protection landscape – 2012 and beyond

For a summary of the data protection developments and the areas organisations should be aware of in the future, please visit the following link:

- http://www.regulatorystrategies.co.uk/assets/pdfs/evolving-data-protection-landscape.pdf

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

Information Commissioner's Office states that private sector leads the way on data protection compliance

The ICO has published a number of reports which show that the private sector is taking a positive approach to data protection compliance. However it has highlighted that there remain serious concerns about compliance in the NHS and public sectors.

The reports summarise the findings of over 60 audits carried out by the ICO between 2010 and 2012 across private, NHS, local and central government sectors. 11 out of 16 audits, conducted within the private sector, have provided the ICO with a high level of assurance about compliance. Organisations within the private sector are audited at the request of the organisation in question. A spokesperson for the ICO stated:

"The private sector organisations we have audited so far should be commended for their positive approach to looking after people's data. However, this does not mean that businesses in the UK should rest on their laurels. We are still seeing relatively few companies agree to an ICO audit and further improvements can be made, particularly, when it comes to the retention or deletion of data."

Health service and government audits generally provided a far lower level of assurance. The reports have resulted in the ICO requesting an extension to its compulsory audit powers to cover NHS and local government sectors.

Organisations warned to encrypt data

Further to the ICO issuing a monetary penalty to Stoke-on-Trent City Council, the ICO is reminding organisations of the need to encrypt sensitive personal information when it is being stored or sent electronically.

The Stoke-on-Trent penalty resulted from sensitive information about a child protection legal case being sent to the wrong person by email. This incident was in addition to a previous undertaking signed by the authority in 2010 relating to the loss of a childcare case stored on an unencrypted USB stick.

The ICO has stated:

"If this data had been encrypted then the information would have stayed secure. Instead, the authority has received a significant penalty for failing to adopt what is a simple and widely used security measure."

ICO's view on the draft Communications Data Bill

The Information Commissioner gave evidence at Parliament's Joint Committee on the draft Communications Data Bill on the 16th October 2012.

Christopher Graham, The Information Commissioner, stated that it is questionable whether the Bill's objective – to provide access to communications data for law enforcement purposes – is achievable. The Bill would provide the ability to monitor up to 85% of communications data but Graham felt that this would simply result in criminals using smaller communications providers. He stated that *"... this would be a system to catch the incompetent criminal".*

Graham also stated that there needed to be serious consideration about what the ICO's role would be. While many additional responsibilities are outlined in the Bill, no additional powers are provided. Graham said that the ICO would require specialist staff, grant-in-aid and the power to audit private sector companies.

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

Definition of personal data

The EU Article 29 Data Protection Working Party is seeking a broad definition of personal data in the draft EU data protection regulations.

The group is suggesting that identification numbers, location data, online identifiers (eg cookies or IP addresses) or other specific factors should usually be considered as personal data.

The wording in the proposals does not currently state that these types of data always need to be considered as personal data.

Recent data protection breaches

Stoke-on-Trent City Council

Stoke-on-Trent City Council has been fined £120,000 as a result of emailing details of a child protection legal case to the wrong person. The recipient of the emails also failed to respond when asked to delete the messages. The council had failed to provide their legal department with encryption software and had not provided appropriate training.

Greater Manchester Police

The ICO has imposed a Civil Monetary Penalty of £150,000 (reduced to £120,000 owing to early payment) on Greater Manchester Police. This resulted from failure to take appropriate measures against the loss of personal information. A memory stick containing sensitive personal information was stolen from an officer's home with details of thousands of individuals linked to serious crime investigations.

Norwood Ravenswood Limited

A monetary penalty of £70,000 has been imposed against Norwood Ravenswood Limited – a social care charity. A social worker working for the charity left detailed reports about the care of four children outside a home. The reports contained information about neglect and abuse as well as information about their birth families.

The ICO had warned charities in August this year that they are potentially more at risk of serious data breaches because of the sensitive information they handle.

Allied Irish Bank

Allied Irish Bank (AIB) informed the Irish Data Protection Commissioner that it had frequently misreported the performance of some of its customer's accounts to the Irish Credit Bureau (ICB). The Deputy Commissioner stated that this was a serious breach of data protection law and the Commissioner is concerned that this incident may not be isolated to AIB and is beginning a generalised audit of financial institutions. The Commissioner is also urging customers to obtain copies of their credit reports.

Bank of Scotland

The Bank of Scotland has been fined £4.2 million, by the Financial Services Authority, for failing to keep accurate records of mortgage payments made by Halifax customers. The bank did not have systems in place to identify which customers were subject to a 'cap' on their standard variable rate.

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

EU update

RegulatoryStrategies

NEWGATE

www.newgatepr.com

The below provides an EU update from a Regulatory Strategies' partner, Newgate Public Relations, in Brussels, and provides an insight into the progress of the EU's draft data protection regulation:

Update on the data protection framework

This month European politicians and national justice and home affairs ministers began to get to grips with fleshing out the details of the new European data protection framework. On the Parliamentary side, a joint meeting was held between European and national MPs to provide a steer to the draft report which the responsible MEP Jan Philipp Albrecht is expected to present in December.

While MPs generally congratulated the Commission for taking a harmonised approach to tackle the current patchwork of data protection laws in Europe, many called for clarity on a number of key issues including the definition of "consent" and "privacy by design and by default".

The Dutch MP Esther Kramer was particularly vocal on the special treatment granted to SMEs, stressing that the criteria for exempting SMEs should be based on the amount of data handled rather than on the number of their employees.

Speaking for the industry, Microsoft strongly advocated the need for a single, coherent framework which could provide clear responses to businesses. Its motto was 'Trust and Transparency' and it also called for the need for incentives and rewards for businesses that demonstrate compliance. Microsoft stressed that the Regulation must provide a clear definition of the "main establishment" and for good implementation of the "one stop shop" mechanism as businesses need to deal with a single authority, especially in cases in which they are simultaneously processor and controller. Businesses also need penalties to be predictable and the uncertainty surrounding the term 'negligent' could jeopardise this.

Representing consumers, the European consumer organisation BEUC stressed that the sanctioning mechanism must be complemented by the introduction of a binding EU instrument for judicial collective redress which would allow data subjects to obtain compensation for the damages suffered..

The shape of the future work in the European Parliament and in the Council is now likely to be set in the course of the coming months, and now is a key time for businesses to provide views to decision-makers on the way forward on the potential impact of the legislation.

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

Data Retention Directive

This month MEPs engaged in a highly charged debate with European Home Affairs Commissioner Cecilia Malmström over the future of the Data Retention Directive.

The existing Data Retention Directive of 2006 requires Member States to ensure that telecoms service providers retain certain categories of data for the purpose of the investigation, detection and prosecution of serious crime. Providers of fixed network and mobile and internet telephony and email are currently required to retain traffic and location data generated or processed and to retain traffic data necessary to identify the sender, recipient, date, time and duration, type, equipment of communication, and, for mobile telephony, the location of the equipment for a period ranging from six months to two years, depending on the national law. Compliance costs are substantial, estimated at around €375 000 in the first year for an internet service provider.

In the Parliamentary debate, the Home Affairs Commissioner insisted during the debate that data retention was needed to protect people from harm, but also admitted that there are a number of areas in the Directive which would need to be improved, and that a revised Directive should include:

- a reduced and harmonised retention period
- clear scope of the types of data to be retained
- minimum standards for access and use of data
- stronger data protection
- a consistent approach to reimbursing operators' costs

While the Commissioner declined to propose a new timetable during the discussion, we anticipate that the Commission will launch internal steps towards a revision of the Directive in the early part of 2013, and that businesses affected by the legislation could reap the benefits of early engagement with decision-makers to improve the current regime.

Visit our website at www.regulatorystrategies.co.uk

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