RegulatoryStrategies

UK Data Protection Newsletter December 2012

Headlines this month:

- Consultation on subject access code of practice
- Consultation on the ICO plan
- Leveson report
- Draft Communications Data Bill
- Binding Corporate Rules for processors
- ICO cookie report
- Ireland's Data Protection Commissioner to enforce cookie law
- Recent data breaches
- EU update

Commentary:

Consultation on subject access code of practice

The Information Commissioner's Office has launched a consultation on a new draft code of practice to assist organisations when responding to subject access requests. It also seeks to support individuals in obtaining copies of their personal information.

The ICO has handled nearly 6000 complaints, in the last financial year, from individuals who are unhappy with the way their subject access requests have been handled. This is higher than any other type of complaint. The final version of the code is intended to make clear exactly what an organisation's legal responsibilities are and what an individual's rights are under the Act. The closing date for the consultation is 21st February 2013 with a view to publishing the code in April 2013.

David Smith, Deputy Commissioner and Director of Data Protection, said:

"At a time when organisations are collecting more and more of information about us, whether online or offline, subject access requests play an increasingly important role in helping us take control of our personal information. They can also benefit organisations by highlighting inaccuracies in their records and giving them the opportunity to update the information they keep about us."

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

The draft code states that an organisation with a positive approach to subject access might use the following indicators of good practice:

- Subject access training to all staff as part of an induction and logged on a database monitored by training staff. Refresher training would be delivered either as part of generic data protection training or in a more specialised way depending on job role
- A dedicated data protection page available to staff via the intranet with links to subject access policies and procedures
- A specific person or team in place to handle requests. There should be more than one person who is aware of how to respond to a request and processes should be in place for a senior manager to review a request where an individual is not satisfied with a response
- Large organisations should have data protection experts to provide expertise including subject access advice within departments where personal data is processed
- Compliance with subject access requests should be monitored and discussed at Information Governance Steering Group meetings. Management information should be kept showing the number of requests received

Consultation on the ICO plan

The ICO has requested the views of the public and stakeholders in its 2013-2016 plan. The closing date for the consultation is 31st January 2013.

The draft ICO plan outlines its goal, vision and mission as follows:

- All organisations which collect and use personal information do so responsibly, securely and fairly
- All public authorities are open and transparent, providing people with access to official information as a matter of course
- People are aware of their information rights and are confident in using them
- People understand how their personal information is used and are able to take steps to protect themselves from its misuse

Leveson report

The ICO issued a statement in response to Lord Justice Leveson's report, published in November 2012. The report criticised the ICO for failing to act upon journalists' attitude to data laws a decade ago and called for data protection legislation to be tightened in the future.

The ICO stated that the report has much for it to consider and that it would reflect on where improvements can be made in the way it carries out statutory duties. It welcomed the fact that the report supported stronger sentences for people who steal or illegally trade in data. However, its view is that the impact upon press would be minimal because journalists would have an enhanced public interest defence available to them.

The report proposes changes to some parts of the Data Protection Act which the ICO see as matter for the Ministry of Justice to consider. However, the ICO will be offering its views on the detail and effects of the proposals in a response to the Leveson Report early in 2013.

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

Draft Communications Data Bill

The Home Office published the draft Communications Data Bill in June 2012 with a view to close what is seen as a gap in the way criminal justice organisations can monitor communications. The Bill requires communications firms and other businesses to store greater amounts of individuals' communications to give more surveillance opportunity to investigators.

The Draft Communications Data Bill Joint Committee has now issued its first report on the Bill stating that plans need a great deal of revision to prevent an impingement of privacy. It also states that the government may have underestimated the cost burdens which could be imposed.

Christopher Graham commented on the report:

"As I have said throughout this process, it is ultimately for Parliament to judge the proposals contained in the draft bill.

My concern is around the adequacy of the proposed safeguards that the ICO would be responsible for regulating. Ensuring the security of retained personal information and its destruction after 12 months would require increased powers and resources, and as it stands today we've not been given clear advice on where that will come from".

Graham goes on to say that the ICO is ready to work with Government to discuss how safeguards can be revised and how they can be made effective.

Binding Corporate Rules for processors

Binding Corporate Rules for processors have been made available for use from 1st January 2013 in order to facilitate international data transfers. The intention of using BCR is to ensure privacy in international transfers bringing benefits to both data controllers and data processors.

The EU Data Protection Authorities' Article 29 Data Protection Working Party has decided to launch this system but makes clear that using BCR for processors is not obligatory. However, once a BCR has been approved, there is no need to negotiate safeguards each time a contract is entered into.

ICO cookie report

The ICO issued a report on the 19th December concerning cookie compliance. It has been encouraging members of the public to report their concerns since May 2012 and between May and November it received 550 reports.

The EU Data Protection Authorities' Article 29 Data Protection Working Party has decided to launch this system but makes clear that using BCR for processors is not obligatory. However, once a BCR has been approved, there is no need to negotiate safeguards each time a contract is entered into.

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

Ireland's Data Protection Commissioner to enforce cookie law

Ireland's Data Protection Commissioner, Billy Hawkes, has written to 80 websites asking what steps they have taken to comply with the cookie legislation. The organisations concerned include Vodafone, Marks and Spencer, PC World, Ryanair, Aldi and Ticketmaster.

The Irish Deputy Commissioner, Gary Davis has stated:

"This is a legal requirement now for 18 months and we are disappointed with the response of websites. Levels of compliance would appear to be very low compared to the UK for instance and we cannot allow that situation to continue. As a first step websites need to provide prominent and clear information to users as to what data they are collecting or allowing to be collected via cookies on their site.

At a minimum this will begin to educate users as to the scale and type of data collection taking place and then better position users to take informed choices as to what cookies they wish to allow or block."

The Commissioner's letter was sent on 19th December 2012 and the websites have 21 days in which to respond.

Recent data protection breaches

The Information Commissioner's Office has criticised local government's attitude towards protecting individuals' personal data further to four local councils being issued with monetary penalties:

Leeds City Council

Leeds City Council sent sensitive personal details about a child in care to the wrong individual and was fined £95,000. The council reused external envelopes to send internal mailings and, in this case, the external address was not deleted.

Plymouth City Council

Highly personal data was sent to the wrong recipient relating to parents and children involved in a child neglect case. The two cases were mixed up when details were sent to a shred printer. Plymouth was fined £60,000.

Devon County Council

A social worker sent an old adoption panel report in error after using the original report as the template for a new report. The report contained details of 22 people including alleged criminal offences and mental and physical health details. Devon was fined £90,000.

London Borough of Lewisham

London Borough of Lewisham was issued with a fine of £70,000 after a social worker left sensitive documents on a train. The documents included GP and police reports and allegations of sexual abuse and neglect.

Christopher Graham, the Information Commissioner, stated:

"We are fast approaching two million pounds worth of monetary penalties issued to UK councils for breaching the Data Protection Act, with nineteen councils failing to have the most straightforward of procedures in place.

It would be far too easy to consider these breaches as simple human error. The reality is that they are caused by councils treating sensitive personal data in the same routine way they would deal with more general correspondence. Far too often in these cases, the councils do not appear to have acknowledged that the data they are handling is about real people, and often the more vulnerable members of society."

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

The ICO continues to press the Ministry of Justice for stronger powers to audit local councils' data protection compliance. The same powers are sought for NHS bodies across the UK.

Barclays bank employee

A Barclays bank employee has been fined after accessing bank statements relating to her partner's ex-wife. Her partner was involved in a dispute relating to a divorce settlement. The employee pleaded to 11 offences under the Section 55 of the Data Protection Act and was fined £500, a £15 victim surcharge and £1,410 prosecution costs.

Christopher Graham commented:

"High street bank staff have access to financial information on a day-to-day basis, and are expected to treat that privilege with professionalism. When that trust is abused and the personal data they access is misused, the law is very clear, as this case has shown."

The Information Commissioner goes on to express his view that the penalties associated with an offence under Section 55 are inadequate. A financial penalty of up to £5,000 can be imposed in a Magistrates Court or a Crown Court can issue an unlimited fine. The ICO still seeks increased deterrents including potential imprisonment. Christopher Graham continued to comment:

"This case illustrates the need for more effective deterrent sentences to be available to the courts, as recommended most recently by Lord Justice Leveson. Unlawful access to personal information is all too easy and all too common - and these days it does not seem to have much to do with the press."

EU update

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:

RegulatoryStrategies

NEWGATE

www.newgatepr.com

Update on the data protection framework

This month policy makers and stakeholders took part in an intensive debate during the Data Protection Conference which took place on 4 December in Brussels.

Many stakeholders raised questions as to whether:

- the removal of general notification requirements for companies goes far enough, or requirements such as the appointment of compulsory Data Protection Officers would represent an increased administrative burden in real terms,
- the fines proposed by the Commission represent the right way to prevent data security breaches and how will compliance be monitored,
- the "one-stop-shop" approach will ensure a harmonised system that protects citizens whilst keeping the administrative burden on industry to a minimum, or will this encourage Forum Shopping,
- the new rules give citizens greater control over their personal data, and how far will proposed measures such as privacy by design and privacy by default go in restoring consumer confidence.

Commissioner Reding in her appearance at the Conference declared her intention to do everything in her power to support the Irish Presidency and the European Parliament "To deliver what business wants. To deliver what citizens want. And to bring European data protection rules into the digital age." She added that: "I trust that together, we will make a giant leap forward for the Digital Single Market. We are closer than ever to delivering effective, practicable and future proof data protection rules that enable growth.

However, she recognised that to make the giant leap a number of further steps need to be taken in the course of the negotiations:

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

Further cuts in red tape

She expressed her willingness to consider building an approach into the legislation that adequately and correctly takes into account risk. As complex analyses of risk may lead to increased costs and less legal certainty, she called for carefully choosing the criteria to be introduced.

Another change she is willing to make is to reduce prescriptiveness in the Regulation. By doing this intelligently, the legislation will remain clear and effective, but at the same time businesses will avoid unnecessary costs.

Further reconciling flexibility and legal certainty

The way the Commission tried to tackle this was to include delegated and implementing acts.

Delegated and implementing acts were never meant to be a way of re-writing the whole Regulation. Although she believes that delegated and implementing acts are one of the ways to achieve legal certainty, she said she is prepared to look at other ways to ensure an effective application of the rules.

Delegated and implementing acts have been re-examined one-by-one. As a result of this exercise, there are a number of delegated and implementing acts that will be replaced by in turn including more detail in the text, allowing the consistency mechanism to step in and make a decision, allowing codes of conduct and other business-lead initiatives or just deleting the act in its entirety.

Speaking in the debate, the German Green Rapporteur for the Regulation Jan Philip Albrecht confirmed the importance of the issue for the Irish Presidency and that Council is willing to negotiate with the Parliament. In describing his approach to the regulation, he said that it aims at better harmonizing and implementing existing rules, strengthening individual rights, as well as creating a single legal framework that is reliable and legally certain.

On the Council side, the Cypriot Presidency issued a note whose purpose was reporting to Member States on the progress achieved on the data protection package. Amongst the concerns expressed, the conclusion emerging from the discussion on the **use of delegated and implementing acts** was that until the first complete reading of the text is finalised, Member States are not in the position to agree alternatives to be adopted in those cases.

On **administrative burdens and compliance costs,** many Member States seem to agree on the need of introducing a 'horizontal clause' in the Regulation, and in particular on the controllers and processors' responsibility, enshrining the risk-based approach. At the same time, Member States agreed that such a clause needs to be accompanied by the introduction of specific risk-based elements in certain provisions.

There is general consensus among delegations that this SME exception is not an optimal solution in all cases. The Presidency has invited Member States to give their views on alternative ways of reducing administrative burden while maintaining the necessary level of protection of individual rights.

In terms of timing, the Parliamentary reports will be presented to the LIBE Committee on 10 January and deadline for amendments will run until end of February.

Now is the right moment for interested organisations to express to MEPs, Member States and the European Commission their views on the key provisions affecting their businesses, as discussion is in earnest and legislation is taking shape.

Visit our website at www.regulatorystrategies.co.uk

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