RegulatoryStrategies

UK Data Protection Newsletter September 2013

Headlines this month:

- Greater coordination of global data protection enforcement
- ICO reaction to Education Secretary's comments
- Calls for change in law to prevent nuisance calls
- Mobile phone gaming apps
- Recent data breaches
- EU update

Commentary:

Greater coordination of global data protection enforcement

The Information Commissioner's Office has won a resolution in Warsaw to lead to greater coordination between global data protection and privacy authorities.

Christopher Graham is the co-chairman of the International Enforcement Coordination Working Group (IECWG) and reported on its work at a recent conference. Christopher Graham commented:

""Data protection has to be effective across borders. The service providers today are often global players. The applications know no borders. The data protection regulatory community can only be effective if we work together across jurisdictions.

"We are making great strides forward in enforcement coordination. The Warsaw conference saw further progress on this vital task".

The ICO has summarised that the resolution seeks:

- That the IECWG works with other networks to develop a common approach to cross-border case handling and enforcement. This intends to address the sharing of enforcement related information
- To encourage privacy enforcement authorities to look for opportunities to cooperate in certain cross-border investigations
- To support the development of a platform offering 'safe space' for enforcement authorities to share confidential information

CO reaction to Education Secretary's comments

The ICO has responded to a recent Daily Telegraph article where Michael Gove, the Education Secretary, suggested that Ofsted were unable to share information with the police to protect children in care.

Christopher Graham commented:

"Ensuring that vulnerable young people are properly protected in care homes is essential. There is nothing in data protection legislation that is a barrier to this happening. This law covers information about people so it has no bearing on the disclosure of non-personal information like the location of care homes.

"If anyone has serious concerns about an individual, either as a potential victim or a perpetrator, then this can be passed on to the police without breaching data protection law."

Calls for change in law to help prevent nuisance calls

The ICO is urging MPs to change the law to help prevent the number of nuisance calls. It is asking the Culture, Media and Sport Select Committee to enable the ICO to issue more monetary fines to companies responsible to these calls.

Currently, the law requires the ICO to prove that calls are causing substantial damage or substantial distress in order to issue a monetary penalty. It can therefore only target companies which are responsible for a large number of calls but it believes that problems are caused by a large number of companies which are making hundreds rather than thousands of calls.

The ICO has presented a business case requesting that the government reduces the amount of harm it needs to prove in order to simply prove 'annoyance or nuisance' before acting.

The ICO stated:

"The simple fact is that the law only allows the ICO to take action against the worst offenders.

"A change in the law would allow us to target more of the companies making these cold calls and would have a noticeable effect for consumers."

The ICO stated:

The ICO has quoted complaint figures showing that 982 companies prompted complaints to the Telephone Preference Service in June about cold calls. 82% of the companies received fewer than five complaints. Only 21 companies received more than 25 complaints.

The ICO has issued clear and detailed Direct Marketing guidance. Its key points are as follows:

- Marketing companies will typically need consent to send people marketing material or pass on details. The fact that consent was knowingly given needs to be demonstrable, that it was communicated in a clear and specific way and records should be kept. Opt-out boxes should be used where possible
- Rules on calls, texts and emails are stricter than for mail marketing and consent should be more specific. A generic approach should not be taken
- Rigorous checks should be taken prior to reliance on indirect consent i.e. consent originally given to a third party. It is unlikely to be valid for calls, texts or emails
- Calls to non-TPS registered numbers can be made but only where it is fair to do so. Specific prior consent must be obtained

- Automated, pre-recorded marketing calls should not be made without specific prior consent
- Marketing or emails should not be sent to individuals without specific prior consent except where there has been a soft opt-in in the case or previous customers
- Neither the Data Protection Act or the Privacy and Electronic Communication Regulations prohibit the use of marketing lists but organisations need to ensure that lists were compiled fairly and reflect peoples' wishes. Bought-in call lists should be screened against the TPS and it will be difficult to use bought-in lists for text, email or automated calls campaigns because these require very specific consent
- The ICO will consider using enforcement powers where an organisation persistently ignores individuals' objections to marketing

The ICO has also issued a checklist for organisations to help make decisions about direct marketing specifically referencing how to obtain consent for marketing, using bought-in lists, making calls and sending texts or emails.

The ICO goes on to comment that:

"Regulatory enforcement isn't and should never be the only solution to the problem. There is a role for the marketing industry to play and for the telecoms companies too. We're working with both to help that to happen...Important too is consumer education - too often we see that apparent nuisance calls have been prompted by consumers ticking a box to give their consent to receive the call."

Mobile phone gaming apps

The ICO has welcomed the report proposing rules to protect children using mobile phone gaming apps particularly in relation to the proposal that developers make clear how and why their app is collecting personal data.

The ICO champions the education of children and questions where a child can read information and make an informed decision about the use of their data in the same way an adult can.

The ICO commissioned lesson plans earlier in the year to educate children about the use of personal information and they are working to promote these with teachers.

Recent data protection breaches

Barclays Bank employee

A former Barclays Bank member of staff was fined £3,360 after accessing details of a customer's account. Information was passed onto the customer's partner by the member of staff who was prosecuted under S55 of the Data Protection Act.

Stephen Eckersley, the ICO's Head of Enforcement, has said:

"The banking industry has rigorous procedures and safeguards in place to make sure customer's details are kept secure. However banks rely on the honesty and professionalism of their staff to ensure that the privileged access given to their records is not abused for personal gain.

"This case proves, yet again, why we need a more appropriate penalty for the crime of personal data theft. With the law as it stands, this prosecution isn't even recorded on the police national computer which means that an offender could apply for a job in a high street bank tomorrow and the potential employer wouldn't be information about the offence. The current 'fine only' regime is clearly not deterring people from breaking the law"

Jala Transport Limited

Jala Transport Limited, a loans company, has been fined £5,000 after the loss of a hard drive containing financial details relating to all its c250 customers. The hard drive was stolen from the business owner's car. The hard drive was password protected but not encrypted and included name, date of birth, address and identity documents,

The ICO states that it expects all data to be encrypted where the loss of data could lead to those affected suffering damage or distress. The limited financial resources of the company meant that the penalty was lowered from what would typically be a fine of £70,000.

The ICO commented:

We have continued to warn organisations of all sizes that they must encrypt any personal data stored on portable devices where the loss of the information could cause clear damage and distress to the customers affected."

Cardiff City Council

An undertaking has been issued to Cardiff City Council further to its failure to respond to a Subject Access Request within 40 days. The ICO consequently looked more closely at the council's SAR compliance and has required:

- Clearly defined procedures for handling requests making sure that staff are fully trained in following them
- Appropriate checks and supervision to ensure that third party data is dealt within in accordance with the Data Protection Act and the organisations policies and procedures
- Sufficient measures are in place for the storage of paper records to make sure requests are handled appropriately

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:

The reform of the data protection framework was high on the political agenda in September, with only one month to go until the European Parliament's lead committee is due to vote on the package, which will mark a key step in the process towards the final legislation.

The European Parliament's Rapporteur, responsible for steering the legislation, German Green MEP Jan Albrecht said in an interview to the EurActiv news portal that the most important goal is create a single framework on data rules that would clearly state what are the rights and obligations for everybody and to distinguish what is one's own data and what is data that is open for use by the industry.

The issue of sanctions is also a key issue for the industry, which was raised this month by the European Commission's Vice President and Commissioner for Justice, Fundamental Rights and Citizenship Viviane Reding. She re-stated her commitment to ensuring that sanctions were included in the final legislation, saying that the tough sanctions (up to 2% of a company's annual global turnover) were needed to make sure that companies comply with EU law. Reding's comment was well timed to coincide with discussions on sanctions in the Council's working group at the end of September.

An issue which continues to divide the Rapporteur and Commissioner, which could yet delay agreement on the whole package, is a possible linkage between data protection and the EU-US Free Trade Agreement. While

Mr Albrecht strongly believes that the trade issues and standards on data protection should be negotiated together, Mrs Reding's opinion is that data protection is a fundamental right and of different nature to the trade issues and that the two should remain separate.

One point on which all the main institutions agree is the need to move more quickly with the package, to have it finalised before the European Parliament elections in May 2014. However, a number of industry representatives, including Intel and Microsoft, and as well the UK's Information Commissioner Christopher Graham, have expressed concern about hurrying with the reform and pushing through a package where the definitions are still unclear and which is not properly thought through.

Beyond the data protection reform package, three other issues of potential interest to the industry were raised in September.

Firstly, a report commissioned by the European Parliament and written by former Microsoft Chief Privacy Adviser Caspar Bowden was launched on 24 September. The report found that US-EU Safe Harbor Framework fails to prevent against U.S. interception of European citizens' cloud-processed data. Therefore, Bowden calls on the Parliament to consider re-instating a deleted article from the initial proposal that would prohibit third countries from accessing personal data in the European Union without prior authorization from a European data protection authority. In addition, he recommends the EU to encourage the development of local cloud computing capacity based on open source software.

Secondly, MEPs demanded that the data-sharing agreement with the US should be suspended. Home Affairs Commissioner Cecilia Malmström said that she had requested formal consultations with the U.S. under Article 19 of the TFTP agreement — a first step toward suspension of the deal.

The third point raised by MEPs was protecting consumers and regulating the so-called "IP-tracking" systems of some commercial Internet sites, used by low cost airlines in particular.

Commissioner Reding responded that it is a matter for the national authorities where Commission's hands are tied. However, if Member States start adapting their national legislation to this particular issue, the Commission might be forced to reconsider the issue and streamline national laws into a European one.

October should finally bring the vote on the data protection package in the Parliament's Civil Liberties, Justice and Home Affairs Committee. The Rapporteur is optimistic that the vote will take place on 21 October and hopes that Council will be ready by the same time, to ensure that the final vote on a negotiated solution can be taken by the end of the Parliamentary term. Now is a key opportunity for businesses to make their voice heard before the vote, which will mark a significant step on the road to finalising the legislation.

Visit our website at www.regulatorystrategies.co.uk

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