RegulatoryStrategies

UK Data Protection Newsletter November 2013

Headlines this month:

- 2020 vision for information rights
- Tribunal overturns ICO fine
- Temporary workers require data protection training
- Scottish referendum campaign groups must comply with marketing rules
- Recent data breaches
- EU update

Commentary:

2020 vision for information rights

The ICO is focussing on how its office may look in 2020 and how it can prepare for an ever-changing landscape. It has therefore opened a consultation on its vision for the next five year which has now been published.

Christopher Graham, the Information Commissioner, stated:

"We need to prepare for a future which is different and ever changing, and, for that reason, we need to become more agile. We need to maintain a strategy approach and be able to adapt within that strategy - not improvise around a series of tactical responses.

"That is what frames the vision we set out today. It's a vision that addresses the growing importance of information rights in the public mind and the impact that has on our workload but against the backdrop of a funding crunch that stretches our resources to the maximum."

The Information Commissioner has outlined three key challenges: Information rights are growing in importance prompted by developments in technology, business and public policy meaning the ICO is increasingly busy; it is facing a funding challenge as resources are being stretched; the regulatory framework is undergoing significant change but the details are not finalised and neither is the timetable against which it will be implemented.

The ICO has proposed the following five aims over the next five years:

- Educating organisations about their information rights obligations; influencing advice provided at EU level on the new legislation;
- Empowering individuals by providing help and guidance to understand their rights
- Enforcement in a proportionate way collaborating with other regulators where appropriate and giving focus to the Privacy and Electronic Communication Regulations
- Enabling action to be taken in the public interest i.e. preventing regulation from being used as a block in appropriately
- Engaging with technology, business and policy developments locally and internationally influencing developments in the European data protection framework, Open Data and big data, transparency, new digital services and global information rights challenges

The ICO stresses that it intends to be outcome focussed. Focussing on outcomes is an area that it has previously stated should be important in the new regulatory framework. It wishes to balance taking formal and informal enforcement action.

Tribunal overturns ICO fine

A fine imposed by the ICO on Mr Christopher Nieble, trading as Tetrus Telecoms, has been overturned by a First Tier Tribunal. The fine had been issued for sending unwanted text messages.

In order for the ICO to be able to issue a monetary penalty, the breach must be deemed serious and also likely to cause substantial damage or distress. The Tribunal assessed that this was not the case.

Temporary workers require data protection training

The Information Commissioner's Office has warned employers that they need to ensure that temporary staff who handle personal data need to receive sufficient data protection training.

The problem of inadequate training was highlighted further to four data breaches at Great Ormond Street Hospital for Children NHS Foundation Trust where letters were sent to incorrect addresses including details about the treatment of five patients. Three of the errors were attributed to temporary staff who had not received data protection training.

The ICO Enforcement Manager stated:

"This time of year often coincides with a rise in the number of temporary workers being employed across the UK. However the temporary nature of their employment doesn't absolve employers of their legal responsibilities for making sure people's information is being looked after correctly.

"If organisations are employing temporary or agency workers into positions that involve the handling and sending out of personal information then they must make sure these staff have received adequate data protection training."

Scottish referendum campaign groups must comply with marketing rules

The Information Commissioner has made clear that Scottish referendum campaigns must comply with electronic marketing rules in the lead up to next year's vote on 18th September 2014.

The warning came after the campaign group, Better Together, signed an Undertaking after sending 300,000 text messages to individuals without checking whether they had given consent to be contacted. The Privacy and Electronic Communications Regulations require organisations to gain an individual's consent prior to sending marketing text messages.

The ICO Assistant Commissioner for Scotland, Ken MacDonald said:

"The Scottish referendum is an important issue, and we understand why both sides of the debate want to communicate with potential voters. But it is absolutely crucial that they continue to do so in a manner that respects rules that exist to protect consumers".

Recent data protection breaches

ICU Investigations Limited

Two private investigators have been prosecuted further to unlawfully obtaining personal information. Five other employees of the same company had already pleaded guilty.

ICU Investigations worked to trace individuals primarily for debt recovery purposes. The organisation had tricked TV Licensing, GPs and utilities companies into revealing personal data. Its clients include Brighton and Hove Council, Allianz Insurance PLC, Leeds Building Society and Dee Valley Water although no criminality was found by the companies employing the investigators. An investigation found 2,000 separate offences.

The ICO Criminal Investigations Team Manager commented:

"Private investigators must learn they are not above the law. While the majority of private investigators go about their business in an honest manner, unscrupulous operators such as ICU Investigations Limited taint the industry and blight the reputations of their counterparts."

Unlawfully obtaining or accessing personal data is a criminal offence under Section 55 of the Data Protection Act by fine only. Christopher Graham stated:

"Public confidence in the security of information held about them is the foundation on which all sorts of online services and developments depend.

"The public expects to see firmer action taken against people who break the rules in this area and Parliament needs to recognise that. I spoke with the Home Secretary, Theresa May, on this matter earlier this week to urge her to introduce more effective sentences for these kinds of offences and she has agreed to meet me to discuss the matter. That conversation needs to result in action"

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

General Data Protection Reform

With the vote of the proposed data protection regulation on 22 October 2013 by the Civil Liberties Committee of the European Parliament, the necessary first step for a proposal to become law has been made. Together with the compromise text, the LIBE Committee adopted a "negotiation mandate" to start official talks with the Council, in view of adopting a joint text.

Adoption of the new Regulation may still be some time away, but the clock is ticking.

The European Council, while concluding that the new Data Protection framework should be adopted in a timely manner in order to strengthen consumer and business trust in Europe's digital economy, did however refuse to commit to adoption by early next year.

France and Poland are said to be the most important supporters of the new legislation, with Sweden, the Czech Republic and the UK willing to postpone the adoption of the legislative package until 2015 at the earliest. Germany's role will be crucial in that recent allegations of US services trying to bug the phone of Chancellor Merkel have made Germany's point of view quite decisive.

There are some Member States that will not be easily persuaded that to jump on board quickly. The UK government in particular has already stated that strengthening the data protection law is a good thing, however, there is a debate as to what extent the law should go. It is said that the UK has had a hard time to find a balanced position that reconciles the interests of the commercial sector and the human rights lobby. The UK Minister of Justice confirmed the UK position on the matter:

"The UK Government is seriously concerned about the potential economic impact of the proposed data protection regulation … a further issue is the possibility of stifling innovation through prescriptive and inflexible rules on gaining individuals' consent…"

From an industry perspective, the majority of businesses affected by new legislation deplore this regulation and find it over prescriptive in that it imposes unnecessary administrative burdens on UK businesses at a time when government should be doing the opposite.

In that regard, the Federation of Small Businesses (FSB) made the following remark:

"If you prescribe in too much detail, you do not leave room for industry to develop their own standards or find their own solutions."

Microsoft added a checks and balances argument to the debate in stating that it was "… very surprised to find that a lot of new burdens were imposed on them, without receiving any new rights and new incentives."

According to the Commission and within the current context of the on-going negotiations about the Transatlantic Trade and Investment Partnership, the EU must adopt data protection reform soon to address fears of US surveillance. A novelty contained in the proposed regulation is the explicitly extended application of EU data protection laws to all companies that offer goods and services to European consumers or monitor the behaviour of European consumers. In fact, the geographical establishment of a company and its processing facilities would no longer determine whether EU data protection laws apply.

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

The Commission's ambitions regarding timing have already been hampered by the long and difficult negotiations inside the Parliament and amongst Member States. Although the plenary vote in the European Parliament is still scheduled to take place on 11th March 2014, things are far from being unison.

While Lithuania has kept the data protection reform relatively high on the EU agenda, Greece's announcement on its Presidency priorities for the first half of 2014 did not include the Regulation.

The Council of Ministers meeting scheduled for 5th/6th December 2013, which will gather ministers in charge of justice and home affairs, will be an indicator of the Member States willingness to move ahead quickly.

There is still some way to go before the final Regulation is adopted. This lengthy process means there is ample opportunity to influence the various parties involved in the negotiations, as well as to pull together industry alliances to increase the impact of such lobbying.

The Council, with its generally more business-friendly position, is likely to be the most effective target for businesses. Although Parliament has been clear on its strict, human rights-oriented position, established lobbying channels and a commitment to keep the negotiation process more or less transparent mean that lobbying Parliament is an easier and potentially effective route to take.

EU-US Ministerial Meeting

This month data protection issues dominated the meeting between the EU and the US Justice and Home Affairs Ministry on 18 November. Commissioner Viviane Reding, pointed out ahead of the meeting:

"…one fundamental issue has not yet been resolved: a meaningful agreement to give European citizens a right to judicial redress: European citizens who are not resident in the US do not enjoy the right to redress in the U. whenever their personal data are being processed in the US…."

The EU and the US committed to advance rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would facilitate transfer of data in the context of police and judicial cooperation in criminal matters by ensuring high level of personal data protection for US and EU citizens.

After the meeting, the Commission has set out the actions that should be undertaken to restore trust in data flows between the US and the EU.

Visit our website at www.regulatorystrategies.co.uk