RegulatoryStrategies

UK Data Protection Newsletter July 2013

Headlines this month:

Commentary:

Push for new Data Protection Regulation

The EU Justice Commissioner, Viviane Reding, has issued a new appeal for Member States to place the Data Protection Regulation on the agenda of an EU summit in Autumn 2013. Reding is keen to get the data protection package completed before the European Parliament elections in May 2014 after it has suffered a number of delays further to debate about the details of amendments.

Reding said:

"I would find it helpful in the European Council in October, which will deal with the European single market, could address this matter and speed up the work in the Council on this important file."

Delays announced by the European Parliament mean that its vote on the version of the EU Data Protection Regulation will be in September or October 2013.

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

ICO Annual Track Survey

The ICO's annual survey has highlighted consumers continued concern about how organisations protect their data. The survey is commissioned by the ICO on an annual basis and asked 971 organisations and 2,465 individuals about data protection and freedom of information issues. 97% of consumers remain concerned about how organisations pass on and sell their data.

Consumers expressed concern about the way personal information is collected and processed by awareness of the right to see information was high.

Chief concerns regarded organisations sharing information with third parties and how securely information is held.

Protecting personal information was the chief concern among consumers after unemployment.

The survey showed a decline in data protection awareness in businesses particularly in terms of the need to keep personal information secure. Awareness of consumers' rights to see information held about them, awareness of the ICO as an enforcer and the need to notify the ICO of processing has also dropped.

Data Protection Authorities may decide levels of fines

A leaked document from the Irish Presidency of the EU Council of Ministers to the Data Protection Working party showed that the administrative fines to be introduced with new EU data protection regulation may be discretionary if the proposal is adopted.

The document suggests that instead of issued fines of up to 2% of global turnover for serious breaches of the Regulation, supervisory authorities could use their discretion and take factors into consideration such as:

- The financial situation of the organisation
- Any previous infringements
- Action taken by the organisation to mitigate damage to consumers

In less serious cases a warning or nominal sanction may apply.

Optional Data Protection Officers

Leaked EU documents have also revealed that thinking amongst the EU Council of Ministers is that Data Protection Officers would not be mandatory under new regulation. The proposed compromise suggests that DPOs could be mandatory if stipulated by national law.

The Justice Minister, Lord McNally has said proposals from the Irish Presidency to adopt a risk-based approach are welcome.

Joint action plan by Ofcom and the ICO

The Information Commissioner's Office and Ofcom have published a joint action plan to tackle the issue of nuisance calls in order to protect consumers.

Claudio Pollack, Ofcom's Consumer Group Director commented:

"This join action plan serves to cement our partnership with the ICO as we work together to tackle nuisance calls and protect consumers."

Simon Entwistle, ICO Director Operations said:

"Only concerted, joint action can tackle the consumer menace of nuisance calls. This plan shows we mean business and outlines how we will continue our work with Ofcom to tackle the problem".

The plan outlines the following priorities:

- Ongoing targeted enforcement against non-compliance in organisations
- Improved call and message tracing processes to identify those responsible for nuisance calls
- Assessment of the impact of the Telephone Preference Service (TPS) on the level of unsolicited live sales and marketing calls to understand how well this currently works for consumers
- Publication of revised industry guidance on marketing consent to include detailed advice on appropriate methods of consent, limitations of indirect third-party consent, time limits and the need for records of consent
- Updated consumer guidance to prevent nuisance calls

An update of progress will be published early in 2014 and an update on various areas of work will be published directly by Ofcom and the ICO.

The ICO is reviewing all of its guidance in relation to direct marketing under the Privacy and Electronic Communication Regulations and the Data Protection Act aiming to publish fully revised guidance in early September 2013.

The ICO has issued a total of £800,000 worth of monetary penalties to date relating to calls and texts.

ICO guidance on data security

The ICO is understood to be in the process of producing new guidance for organisations on the issue of IT security. The guidance should set out guidelines on the technical measures organisations take to ensure that comply with data protection rules.

The guidance will also explain what a number of organisations which have experienced a data breach should have done differently in order to comply with the Data Protection Act.

ICO update on Google privacy policy

The ICO has a statement in relation to Google after working with members of the Article 29 Working Party relating to Google. It states that they will continue to coordinate activity and other EU data protection authorities issued similar statements. The statement states:

"We have today written to Google to confirm our findings relating to the update of the company's privacy policy. In our letter we confirm that its updated privacy policy raises serious questions about its compliance with the UK Data Protection Act.

In particular, we believe that the updated policy does not provide sufficient information to enable UK users of Google's services to understand how their data will be used across all of the company's products.

Google must now amend their privacy policy to make it more informative for individual service users. Failure to make the necessary action to improve the policies compliance with the Data Protection Act by 20th September will leave the company open to the possibility of formal enforcement action".

Online dating companies

The ICO has written to four of the largest online data companies in the UK after questions were raised about their handling of personal data. A survey of major sites identified areas where the Data Protection Act was not being complied with.

The companies have been asked to respond to who they are meeting concerns relating to:

- Poor visibility of the terms and conditions giving consent to use personal information in certain ways
- The terms and conditions making reference to the companies having 'perpetual' or 'irrevocable' licence to use members' data
- Claims that companies take no responsibility for the loss of or damage to personal data
- The expectation that users provide personal details before terms and conditions are provided

ISP and telecoms data breach notification

The European Commission has announced new technical implementing measures addressing the EU data breach notification requirement for telecom operators and internet service providers. These have been adopted as a Commissioner Regulation and take immediate effect - not requiring implementation into the national law of EU Member States.

Companies must notify its national authority within 24 hours of detection of a breach (or provide an initial description of the breach), outline data affected and the measures that have or will be taken by the company, pay attention the type of data compromised when deciding whether to notify subscribers and use a standardised format for notifying the national authority.

Monetary penalty overruled

The Scottish Borders Council has successfully appealed a fine issued by the ICO in September 2012 after employee pension records were found in a recycling bin. The Tribunal agreed that the breach was a serious one but was not satisfied that it would lead to substantial damage for the individuals affected.

Sony has recently announced that it has dropped its appeal against the ICO's decision to fine it £250,000 for the loss of data relating to millions of UK users.

The imposition of a monetary penalty is based upon the following criteria:

- A serious breach of the Data Protection Principles or the Privacy and Electronic Communication Regulations
- The breach must cause substantial damage or substantial distress
- The breach was deliberate or
- The person in breach knew or should have known that there was a risk that the breach could occur

Recent data protection breaches

Tameside Energy Services Limited

TA monetary penalty has been served on Tameside Energy Services, a Manchester based company, for £45,000. The fine was reduced from £90,000 when the ICO took into account the company's financial circumstances.

The company was found responsible for over 1,000 complaints to the Telephone Preference Service (TPS) and the ICO between May 2011 and January 2013 relating to energy efficiency improvements. One complaint was from a pensioner who complained after asking the company to cease contacting her over 20 times.

The company failed to remove people from their contact lists or to carry out checks with TPS which is a legal requirement under the Privacy and Electronic Communication Regulations. The ICO has also issued an enforcement notice requiring Tameside to stop calling people who have registered with the TPS or asked to be removed from their contact list - failure to comply would result in formal prosecution.

A spokesperson for the ICO stated:

"This is not the first and will not be the last monetary penalty issued by the ICO for unwanted marketing calls. These companies need to listen...

...We are continuing to work with the industry, government and other regulators, including OFCOM, to coordinate our efforts to tackle this problem. We would like to see the law changed to make it simpler for us to punish companies responsible for repeated and continuous breaches of the law."

NHS Surrey

NHS Surrey was issued with a monetary penalty of £200,000 further to the discovery of 3,000 patients' records on a second hand computer purchased on an online auction site.

The information was left on the computer and sold by a data destruction company employed to wipe and destroy computer equipment. After finding the problem, NHS Surrey reclaimed 39 computers sold by the trading arm of the data destruction company - three of which contained sensitive personal information. **The ICO found that there was no contract in place with the new provider and failed to observe and monitor the data destruction process.**

Hertfordshire Constabulary

The ICO has issued Hertfordshire Constabulary with an enforcement notice ordering them to review its use of Automatic Number Plate Recognition (ANPR) cameras.

An ICO investigation showed that there was extensive use of ANPR cameras around the town of Royston meaning that anyone driving in or out of the town would have a record kept of their journey. The scheme is referred to as 'the ring of steel'.

A joint complaint was made by the privacy groups Big Brother Watch, Privacy International and No CCTV.

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

In July, key players in the data protection debate began to harden their positions before the EU institutions move towards decisions on the new framework over the autumn

German Chancellor Angela Merkel demanded stricter EU data protection rules ahead of a Justice and Home Affairs Ministers meeting, saying that "we have a great data protection law here in Germany, but if Facebook is registered in Ireland, then Irish law applies. So we need a unified EU regulation." Mrs Merkel is subject to domestic political pressure on the issue, in advance of the German Parliamentary elections due in September, with opposition representatives blaming her for failing to protect the rights of German citizens.

EU Commissioner for Justice, Viviane Reding, expects the European Council in October, which will deal with the European Single Market, to address the Data Protection package and speed up the work in the Council. She stressed at a recent conference that clear rules and the choice for the individual to give out his data or not are needed. In particular, she highlighted the "one continent, one rule" principle; the inclusion of processors, such as cloud providers, in the scope of the rules; and safeguards against the unfettered international transfer of data.

It is clear that business representatives continue to have significant concerns about the impact of the changes ahead. **A survey by the European Multi-channel and Online Trade Association, which represents about 80% of the online traders in EU showed that, out of 90 European online retailers polled, two thirds say that proposed changes to EU data protection rules will damage business.** The companies feared that the rules will increase costs and negatively affect marketing and consumers' experience of buying online.

Furthermore, 70% of the survey replies showed that companies fear the change will impede first contacts with new potential customers or affect marketing to existing customers. On the requirement to hire a data protection officer, 90% of companies thought it would be too burdensome in running costs.

International aspects of data protection continue to feature strongly in EU debates, further to the PRISM scandal, and this month the European Parliament approved a resolution on the US surveillance programme, which condemned PRISM and spying in the strongest terms, and called for an in-depth European Parliamentary Committee inquiry into the matter, to report by the end of the year. The inquiry will assess the impact of the alleged surveillance activities on EU citizens' right to privacy and data protection, freedom of expression, the presumption of innocence and the right to an effective remedy, with witnesses to include journalists, legal experts and whistleblowers.

In terms of wider repercussions, Socialists and Green MEPs called for the negotiations on the Transatlantic Free Trade Agreement to be postponed and, in the light of the revelations about mass surveillance of communications by the US, German data protection authorities have asked the European Commission to suspend the "Safe Harbor" agreements – designed to allow exchange of personal data with US organisations - and review whether the US companies can still comply with them. EU Commissioner Reding has expressed doubt about the effectiveness of the data protection standards in the agreement and said that "the Commission is working on an assessment of the "Safe Harbor" agreement which we will present before the end of the year."

The orientation vote on the Data Protection package is expected to take place in October and both the Commission and the Parliament are pushing to have the bill completed before the European Parliament elections in May 2014. Given the high degree of controversy of different aspects of the legislation, companies can still influence the outcome of the process by engaging with key stakeholders as the EU institutions reconvene at the end of August.

Visit our website at www.regulatorystrategies.co.uk

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