RegulatoryStrategies

UK Data Protection Newsletter April 2015

Headlines this month:

Commentary:

Data Protection reform

The first draft of the document that will form the final text of the Data Protection regulation has been released showing the text proposed by the European Commission and the version the European Parliament has recommended and the version likely to be recommended by the European Council.

The European Council is looking to reach final agreement by the 15 June 2015.

Organisations will therefore need to start ensuring that businesses are fit to comply with the new regulations – once final agreement is reached there will be two year period prior to full implementation in all EU member states. The Regulations will automatically be applicable as drafted with no room for amendment or interpretation.

Some of the areas which will undoubtedly come into force include:

- Mandatory data breach notification (either within 24 or 72 hours) to both affected customers and to the Regulator.
- Restrictions on profiling which will impact marketing – the Direct Marketing Association has published guidance on how it believes this will affect companies.
- Organisations will be required to have robust

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

policies and procedures in place covering all aspects of Data Protection and these could potentially be audited.

- Any new products or new processing of personal data will be subject to Privacy Impact Assessments and a Privacy by Design culture must be adopted.
- Organisations will need to appoint a Data Protection Officer (DPO) either internally or by contracting with an external specialist (if they employ more than 250 staff or process over 5000 pieces of personal data annually – to be agreed). The DPO must have a level or independence and autonomy.
- Data Processors will have their own direct obligations unlike the current position where they are the responsibility of the Data Controller. This will impact existing agreements and contracts.
- The bar will be raised where consent is relied on as the condition to legitimise processing, with explicit consent being the default position.
- Organisations will be subject to a prescribed level of fines, for data protection breaches, unlike the current position where member states set their own levels of penalty. It is likely that fines will be up to a maximum of 100 million Euros or, for global organisations, up to 5% or annual turnover.

Data Protection reform – a Big Data enabler

The European Commission has published a fact sheet about Big Data and has identified the proposed EU data Protection reform as an enabler for Big Data Services in Europe.

The Commission defines Big Data as:

"... large amounts of different types of data produced from various types of sources, such as people, machines or sensors. This data could be climate information, satellite images, digital pictures and videos, transition records or GPS signals. Big data may involve personal data: that is., any information relating to an individual, and can be anything from a name, a photo, an email address, bank details, posts on social networking website, medical information, or a computer IP address."

The Commission sates that the data protection reform package will build a single, strong and comprehensive set of data protection rules for the EU and will boost innovation.

Opt out consent insufficient

The Data Protection Regulator in Hamburg has said that forcing consumers to de-select pre-ticked boxes when collecting personal information goes against their 'right to informational self-determination'.

The comment was made in light of the latest agreement of EU Ministers on data protection reform. He said that organisations should be required to obtain explicit consent to the processing of personal data when they seek to rely on consent as the legal basis for processing the information. The current agreement was criticised because it would enable organisations to process personal information where they had unambiguous consent to do so.

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

Trade in pension's information

The UK Information Commissioner, Christopher Graham, has said that the trade in individuals' pension data has the potential to be the 'next PPI scandal'.

The ICO has launched an investigation after claims published in the Daily Mail suggested that millions of individuals' data is being sold and ending up in the hands of criminals.

Christopher Graham commented:

"I think it is very serious and we have immediately launched an investigation.

"We are in touch with the pension's regulator, the Financial Conduct Authority and the police because this looks like a very serious breach of the Data Protection Act.

"If it is a breach of the Data Protection Act, then the companies involved are facing serious civil monetary penalties of up to half a million pounds."

Section 55 offences

Magistrates' courts are no longer limited to £5,000 fines for criminal offences under the Data Protection Act. Regulations now allow for an unlimited fine where individuals are convicted under Section 55 of the Act.

Section 55 (1) of the Data Protection Act states:

"A person must not knowingly or recklessly, without the consent of the data controller –

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data".

UCAS application form

The ICO has ruled that people applying for further education were wrongly being sent advertisements about mobile phones, energy drinks and other commercial services and that the Universities and Colleges Admissions Service (UCAS) had broken electronic marketing rules.

The ICO has required UCAS to change its practices after determining that its opt-out options did not offer a balanced choice to prospective students by making them feel that they need to allow their information to be used for commercial purposes in order to obtain important information about careers or education.

The ICO Head of Enforcement said:

"Each year, more than half a million teenagers register with UCAS to apply for a place in higher education. UCAS has a responsibility to ensure that applicants can make free and balanced choices. By failing to give these applicants a clear option to avoid marketing, they were being unfairly faced with the default option of having their details used for commercial purposes. Our guidance is clear that consent must be freely given and specific.

"We are pleased that UCAS has agreed to address this issue and will now update their form so that people can make an informed decision on whether they are happy to receive marketing, or not. This can only be a good thing for our aspiring students by helping them to keep up-to-date on the information they want, while avoiding the hassle of unwanted marketing."

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

Recent data protection breaches

Reactiv Media Limited

Reactiv Media were served with a monetary penalty in July 2014 for making unsolicited calls to people who were registered with the Telephone Preference Service. Reactive Media appealed the decision but the Information Rights Tribunal has overturned the appeal.

The original fine issued to Reactiv Media was £50,000 but the Tribunal has increased this to £75,000. The Tribunal stated that evidence showed 'a culture of denial and minimisation of the breach, weak governance of the company and tendency to blame others rather than accept responsibility'.

British Airways

British Airways have warned frequent fliers that hackers have gained access to a large number of accounts resulting in the disappearance on award points.

A British Airways user was advised that unauthorised activity resulted in a third party using information to obtain access to his Executive Club account.

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:

It seems that the pace of the data protection negotiations will soon speed up as the EU Council has received the message from both the Parliament and the Commission to finalise discussions on out-standing issues. After last month's agreement on the issue of the 'one-stop-shop' mechanism as well as on the principles of the processing of personal data, the Council now seems to be determined to move the Data Protection Reform ahead.

In April, negotiations have been on-going and have led the Council to prepare a general approach on the rights of the data subject (Chapter III of the Regulation), with a deal to be envisaged in the short run.

This chapter is very comprehensive and considered to be the most significant part of the draft Regulation. It has been discussed in its entirety for the first time already under the Irish Presidency in Spring 2013 and it has come back to the forefront of the negotiations with the Google case under the Italian Presidency. Now the Latvian Presidency of the Council is pushing the Chapter to the finish with a compromise suggestion.

Data subjects have several rights, and one of them is the right to be forgotten. Extremely topical at the time when the Court of Justice issued the "Google-case", the Presidency now came up with a compromise that would provide a right to oblige the data controller to erase personal data as well as the right to object the processing of such data.

The UK delegation had continuously referred to the challenge it would bring to make data subjects behave responsibly in an online environment, and whether the right to be forgotten would not be counterproductive, by creating unreasonable expectations as to the possibilities of erasing data.

Data portability, also known as the right to transfer data from one electronic processing system to and into another, without being prevented from doing

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

so by the controller, caused more discord among the delegations. Apart from the fact that they (Denmark, Germany, France, Ireland, Poland, Netherlands and UK) found this rule to be part of competition law and/or intellectual property law rather than data protection law, they feared it would increase the administrative burden for businesses.

The new data erasure rules will force the industry to comply with the new Regulation. Software producers will have to ensure personal data is never exposed to unauthorised users and can always be deleted. According to a major analyst company, the new law requires good if not better identity and access management, which is currently lacking throughout Europe.

This compromise suggestion from the Council's presidency is said to be one of the last hurdles to take before reaching a final agreement at Council in June, before the end of the mandate. In addition to it, the Council will still have to find partial general approaches on a number of open issues, such as e.g. the chapter on remedies, liability and sanctions.

In terms of next steps, the Council is aiming to form its common position by the end of June, thereby paving the way for the trialogue to start before the European Parliament's summer break. These last months are crucial for businesses to lobby in favour of their interests: the major tenet of the negotiating parties at the table is that "nothing is agreed until everything is agreed", which leaves major opportunities for the industry to act until the end of June and thereafter, in the trialogue process.

Visit our website at www.regulatorystrategies.co.uk

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