Data Protection Newsletter

August 2015

Headlines this month:

- Preparing for EU reform
- EU DP Trilogue negotiations
- ICO analysis of the Data Protection Regulation
- Charity data sharing
- Children's websites and apps
- Recent data protection breaches
- EU update

Commentary:

Preparing for EU reform

The Information Commissioner has commented on the progress of EU reform stating that negotiations are going to plan and that we should be well aware of what is in the Regulation by the end of the year. The ICO's prediction is that the Regulation will be in force from June 2018 although possibly later in 2018.

They go on to comment that, while there is time, businesses should be preparing now by making sure that current responsibilities are being met. In relation to the future changes, the ICO has commented on the following:

- **Consent and control**
  Do customers understand what they are consenting to and the implication (particularly where children are involved)? Can they easily withdraw consent?

- **Accountability**
  Are effective processed in place to ensure data protection compliance and are these demonstrable? Can individuals easily find out what is held about them and generally find out about data protection practices in your organisation?

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

- **Staffing**
  There should be the right people in place to allow an organisation to understand and meet the requirements of Regulation. If this is not in place, organisations should identify where resource will come from

- **Privacy by Design**
  Is data protection compliance embedded in systems and processes? Are there reviews about what data is held and is data minimised where possible? Are Privacy Impact Assessments used?

- **Breach management**
  Is there a data breach management process in place and is it ready to be activated? Are measures in place to prevent breaches in the first place?

EU DP Trilogue negotiations

The ICO has commented on the EU Trilogue discussions which will continue to run until December. Reports of the sessions currently run suggest the outcome is positive and efforts are being made to reach a compromise in respect of the draft texts issued by the EU Commission, Parliament and Council.

The ICO has identified various areas to look out for as discussions progress:

- Whether there will be attempts to regulation where there is a conflict between a legal requirement of a non-EU country requiring disclosure of personal data held in the EU to that country and EU data protection law.
- The extent to which processing of personal data can be based on a data controller's 'legitimate interests'
- How much more supervision there will be of international transfers
- Whether data breach notification will take place within 24 hours, 72 hours are "without undue delay"

ICO analysis of the Data Protection regulation

The ICO has issued some detailed analysis of the proposed Data Protection Regulation to reflect its observations on areas where it believes the most improvement is required.

Some of the key observations are as follows:

- There is a risk that different data protection regimes may develop in different locations so any separate arrangements should be kept to a minimum

- It may be difficult for an organisation to evaluate whether processing can be justified in terms of 'legitimate interests'
- There may be confusion about what sort of consent organisations will be required to obtain in view of the references to 'unambiguous' and 'explicit'
- The need to have special protection of children whose data is being processed is acknowledged but it is felt that there is a lack of flexibility and that 'child' is not defined.
- There are concerns about the possibility of receiving high volumes of data breach notifications where they are not 'high-risk'
- The list of qualities and functions of a Data Protection Officer is excessive and will not reflect the way many organisations manage data protection compliance

Charity data sharing

The ICO has launched an investigation to identify issues around data sharing in the charity sector further to recent reports in The Daily Mail.

Christopher Graham has stated:

"The Data Protection Act is very clear: the very first principle is that your data should only be processed fairly and lawfully. What has been described in the papers this week doesn't look like that...

"...The law expects you to bear in mind people's interests and people's expectations. If people say 'I never gave you permission to do that' and you respond 'well, yes you did actually, because in 1994 you forgot to tick a box', then that isn't consent. That doesn't give you the right to trade in people's personal information years after the event."

Children's websites and apps

An international project has taken a look at websites and apps used by children and concerns have been raised about the personal information collected.

The Global Privacy Enforcement Network saw 29 data protection regulators look at websites and apps targeted at children showing that 67% collected personal information about them.

The results showed:

- 31% of sites had effective controls in place
- Half of the apps and sites reviewed shared information with third parties
- 22% provided an opportunity for children to provide their phone numbers
- 58% offered children the opportunity to be redirected to other sites
- Only 24% of sites encourage parental involvement

- 71% of sites did not offer an easy means for deleting account information
-

Recent data protection breaches

The Money Shop

A £180,000 monetary penalty was issued to The Money Shop further to a loss of computer servers containing details of several thousand customers. Servers were lost in two separate incidents. The ICO investigation showed that, while servers should be held in separate locked rooms, this was not the case in many instances. The servers had insufficient encryption to protect personal information.

The ICO's Head of Enforcement commented:

"Customers of the Money Shop entrusted the company with their personal and financial details with the expectation that the information would be kept safely and securely. Our investigations discovered that this wasn't the case and that this information was regularly left exposed when equipment was moved around the country. There was potential for fraud and financial loss to customers which is unacceptable and in both cases, had the data been properly encrypted the damage and distress to customers and monetary penalty could have been avoided.

"Hopefully it's an example to other organisations, whatever business they may be in, that the safety of personal information must be taken seriously. Policies and procedures must be put in place or we will take action".

Carphone Warehouse

Carphone Warehouse reported that its systems suffered a cyber attach placing customers' data at risk. The personal data in question includes names, addresses, dates of birth and bank details relating to up to 2.4 million customers. Credit card data relating to 90,000 may also have breached although this is encrypted.

A spokesperson from the ICO stated:

"We have been made aware of this incident at the Carphone Warehouse and are making enquiries. Anytime personal data is lost there can be a risk of identity theft, for instance being vigilant around items on your credit card statement or checking your credit ratings."

Point One Marketing Limited

Point One Marketing Limited trading as 'Stop the Calls', offering a service to remove people from a cold call database has been fined £50,000 by the ICO as a result of its own aggressive cold calling.

The ICO's Head of Enforcement commented:

"This company lacked integrity. They tried to sell a product that they claimed would stop nuisance calls, knowing full well they were responsible for so many such calls themselves. They operated in what appears to have been such a bullying, aggressive way only makes matters worse."

EU update

The below provides an EU update from Brussels, and provides an insight into the progress of the EU's draft data protection regulation:

While EU legislators were formally on holidays in August, industry lobbying activities and discussions on the EU General Data Protection Regulation (GDPR) continued to ramp up in advance of further negotiations in September.

The Industry Coalition for Data Protection - which represents internet, computer and technology trade associations including major companies such as Apple and Google - sent a letter to the key representatives of the three EU Institutions involved in the GDPR negotiations, namely the European Commissioner for Justice, Consumers and Gender Equality Věra Jourová, MEP Jan Philipp Albrecht, the European Parliament's leading negotiator, and the Luxembourg Presidency of the Council which took over the reins of the Institution representing EU Member States on 1 July.

In their letter, the industry representatives call for the deletion of the European Parliament's proposal for a new Article 43a, according to which non-EU court rulings or administrative orders requiring disclosure of the EU citizens' personal data could only be applied if such judgements or orders are locally binding pursuant to international agreements or a mutual legal assistance treaty, or if local data protection authorities authorise the disclosure. This proposal was introduced in the European Parliament's negotiating text in the aftermath of Edward Snowden's revelations and is informally known as the *'anti-FISA'* clause, referring to the American Foreign Intelligence Surveillance Act which regulates U.S.'s international surveillance activities.

The ICDP accuses the EU of adopting a *'unilateral approach'* which would likely generate conflicts of law and undermine *'both the principles of reciprocity in diplomatic relations as well as the credibility of the EU data protection reform.'* In particular, the industry fears that situations could arise in which one company could be asked by a third-country authority to disclose EU citizens' data but would be forbidden from complying under the GDPR. Moreover, third countries may adopt similar provisions and EU companies operating in those markets would face many problems when dealing with a request from EU national authorities to disclose customers' data. In order to avoid such problems, the Industry Coalition suggested that the EU should address the issue in the Directive which is going to accompany the GDPR and specifically deals with law enforcement issues.

Mr Albrecht, who supports the new Article 43a, strongly rejected ICDP's proposal while Commissioner Jourovà reassured the industry by stating that *'the regulation will provide businesses with more legal certainty'*.

In terms of next steps, a third inter-institutional trilogue meeting will take place in Brussels in early September. Negotiations are expected to become more complex as proposals relating to the rights of the data subject (Chapter III) as well as the principles for protecting the personal data (Chapter II) will be addressed for the first time. As negotiations are likely to last until December 2015, businesses should not hesitate to

continue their lobbying activities since a number of controversial issues are still on the table.