UK Data Protection Newsletter

July 2014

Headlines this month:

- Information Commissioner's Annual Report
- Effectiveness of the Telephone Preference Service (TPS)
- Big Data
- Data Retention and Investigatory Powers Act
- Recent data breaches
- EU update

Commentary:

Information Commissioner's Annual Report

The Information Commissioner Office launched its annual report on 15th July stressing the importance to the general public of having an independent regulator. It warned that independence means having strong powers and sustainable funding.

Christopher Graham, the Information Commissioner, introduced the report by saying:

"Facebook, care.data, Google: it is clear that organisations' use of data is getting ever more complicated. People need to know someone is watching over their information.

"That needs to be someone who's independent, of government and business, so the public know the regulator can be trusted. Sometimes the state is itself the issue. When the Intelligence and Security Committee wanted to know how the Snowden revelations fitted with data protection law, it was the Information Commissioner they turned to.

"Independence means someone who's got the resources to take on this ever-growing number of cases. The last twelve months have been a record year - more complaints resolved than ever, more enforcement action taken and more advice given through our helpline.

"And it also means having the powers to act on the more serious complaints. A strong regulator is needed if a data breach affects millions of people.

"That someone is the Information Commissioner. We're effective, efficient and busier than ever. But to do our job properly, we need stronger powers, more sustainable funding and a clearer guarantee of independence."

Data protection complaints

The ICO received 7.1% more complaints in 2013/14 compared with the previous year totalling 14,738 complaints. 35% of these cases resulted in a 'compliance unlikely' decision; 33% of complaints were treated as 'complaint made too early' (the ICO expects complainants to resolve complaints with the organisation directly in the first instance).

The sectors generating the most complaints were:

- Lenders - 17%
- Local government - 12%
- Health - 10%
- General business - 9%
- Central Government - 7%
- Policing and criminal records - 5%
- Telecoms - 4%
- Education - 4%
- Insurance - 3%
- Retail - 2%

Reasons for complaints were as follows:

- Subject access - 50%
- Disclosure - 17%
- Inaccurate data - 15%
- Security - 6%
- Fair processing - 2%
- Use of data - 2%
- Right to prevent processing - 2%
- Retention of data - 1%
- Obtaining data - 1%
- Excessive / irrelevant data - 1%

Privacy and Electronic Communications Regulations

161,720 complaints were received (an annual decrease of 178) and 278 cookie concerns were raised (a decrease of 407).

45.7% complaints related to automated calls, 18.6% to spam texts and 34.7% to live calls.

Effectiveness of the Telephone Preference Service (TPS)

Ofcom and the Information Commissioner's Office have issued the finding of a study to determine the effectiveness of the Telephone Preference Service. The study (conducted by Ipsos MORI) focussed on whether signing up to the TPS significantly reduced the number of live marketing / sales calls received.

The ICO and Ofcom are sharing the research with Government to help inform its consultation later in the year to make it easier for the ICO to take action against organisations breaking the rules.

Research showed that the TPS is effective in reducing the number of live marketing / sales calls received. The full study can be found at: http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/tps-effectiveness

The ICO issued a News Release on 24th July 2014 reiterating the purpose of the TPS. It also stated that, while the number of nuisance calls reduce when somebody registers with the TPS, too many people continue to receive them.

Big Data

The Information Commissioner's Office has set out how big data must comply with data protection rules in an extensive report. The ICO defines big data as:

"... a way of analysing data that typically uses massive datasets, brings together data from different sources and can analyse the data in real time. It often uses personal data, be that looking at broad trends in aggregated sets of data or creating detailed profiles in relation to individuals, for example lending or insurance decisions".

The ICO report refers to the Gartner IT glossary definition of big data:

"Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making".

The ICO's report details how the law is applicable when big data uses personal information and which aspects organisations need to consider - how organisations can remain compliant but continue to be innovative.

The ICO's Head of Policy has announced the report by stating:

"There is a buzz around big data and emerging evidence of its economic and social benefits. But we've seen a lot of organisation who are raising questions about how they can innovate to find these benefits and still comply with the law. Individuals too are

showing they're concerned about how their data is being used and shared in big data type scenarios.

"What we're saying in this report is that many of the challenges of compliance can be overcome by being open about what you're doing. Organisations need to think of innovative ways to tell customers what they want to do and what they're hoping to achieve."

The report recognises that many examples of big data analytics do not use personal data but cites examples that do involve processing personal data such as social media, loyalty cards and sensors in clinical trials. It references the need to ensure that processing is 'fair' and particularly where big data is being used to affect decisions made about individuals. **Organisations need to be transparent when collecting data and explain how it will be used - the ICO does not see the complexity of big data analytics being an excuse for failing to obtain consent.**

If data has been obtained for one purpose and an organisation decides to analyse the data for completely different purposes (or make it available to others to do so) it needs to make its users aware of this. This is particularly important where the purpose is not apparent to the individual and unconnected with their use of a service.

Some of the considerations the ICO deem important when using big data analytics are as follows:

- **Personal data** - is it essential to use personal data? Can it be anonymised? If it is being used it needs to be processed in compliance with the Data Protection Act
- **Privacy impact assessments** - A privacy impact assessment should be carried out to understand how processing will affect people. Is data being used to identify trends or make decisions that affect individuals?
- **Repurposing data** - If data is being used for a new purpose consideration needs to be given to whether this is compatible with the original purpose or whether consent needs to be obtained. If data is being bought from elsewhere due diligence will need to be undertaken and it should be ensured that there is data protection condition for processing
- **Data minimisation** - Data cannot be stockpiled or kept for longer that needed for the business purpose.
- **Transparency** - Organisations should be as transparent as possible. The purposes, implications and benefits of analytics should be explained.
- **Subject access** - People have the right to see the information being used about them so systems should be designed to make it easy to collate information. Thought should be given to enabling people to access their data on line.

Data Retention and Investigatory Powers Act

The Data Retention and Investigatory Powers Act (DRIP) was adopted quickly in July to force mobile and landline providers and Internet Service Providers to store customers' calls, text messages and emails for 12 months.

Christopher Graham has confirmed that his office has gained new funding from the Home Office and in 2015/16 he expects to recruit another team of auditors. This should monitor affected companies' data collection to ensure retention does not go beyond of the scope of the law.

The new law has replaced the Data Retention Regulators 2009. It makes clear the circumstances under the Regulation of Investigatory Powers Act (RIPA) in which a warrant can be issued. The government has said that the new law does not add more powers and is vital in the fight against crime and terrorism.

Recent data protection breaches

Think W3 Limited

An online travel company has been issued with a monetary penalty of £150,000 because thousands of people's details were revealed to a hacker in December 2012. Nearly half a million current credit and debit cards (plus many expired records) were hacked through a subsidiary company, Essential Travel Limited. No card details had been deleted for six years and no security checks or reviews had occurred.

The Information Commissioner's Head of Enforcement stated:

"This was a staggering lapse that left more than a million holiday maker's personal details exposed to a malicious hacker.

"Data security should be a top priority for any business that operates online. Think W3 Limited accepted liability for failing to keep their customers' personal data secure; failing to test their security and failing to delete out-of-date information.

"The public's awareness of the importance of data protection is rising all the time. Ignorance from data controllers is no excuse. They must take active steps to ensure the personal data they are responsible for is kept safe or face enforcement action and the resulting reputational damage."

Enterprise Rent-A-Car

A former employee of Enterprise Rent-A-Car has been prosecuted by the Information Commissioner's Office after stealing records of almost two thousand customers and selling them to a claims management company.

Unlawfully obtaining or accessing personal data is an offence under Section 55 of the Data Protection Act although it is only punishable by a fine. The Information Commissioner's Office continues to lobby for the ability to impose stricter action and potentially prison sentences.

In this case, the ICO raided the claims management company and recovered the records. The ICO Head of Enforcement commented:

"Data theft is not a victimless crime and many of the people targeted ... will have received nuisance calls offering to pursue a personal injury claim".

Betsi Cadwaladr University Health Board

A Welsh Health Board has been found in breach of the Data Protection Act after sensitive personal information was sent to the wrong address. Eight letters were sent to only one patent. The letters contained details of medical treatment.

The ICO found that the individual responsible had received no data protection training. The health board had introduced mandatory data protection training in April 2013 but by February 2014 only 6.5% of staff had received it.

The health board has signed an Undertaking committing it to improving training and prioritising staff who deal with sensitive personal information.

Reactiv Media Limited

Reactiv Media Limited has been issued with a £50,000 fine after the ICO conducted an investigation showing that they had been making unsolicited calls to individuals who were registered with the Telephone Preference Service. The TPS received 481 complaints and the ICO received 120 complaints.

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:

In July, EU Ministers took a step back from the details of the data protection reform to consider more broadly whether greater flexibility is needed in certain areas. This follows the Justice and Home Affairs Council of 6 June which had led to a degree of compromise on the Data Protection Regulation, and more in particular on the territorial scope, the definitions of "binding corporate rules" and "international organisation" as well as the transfer of personal data to third countries or international organisations.

At an informal meeting in Milan on 8-9 July, chaired by the new Italian Presidency, the Justice and Home Affairs Council discussed whether there should be greater flexibility within the proposed General Data Protection Regulation for Member States to provide a higher standard of data protection for the public sector at national level. Various approaches were discussed, including one that would provide for specific exemptions throughout the text of the proposed Regulation. The UK argued that the best way to achieve the desired flexibility was to legislate by way of a Directive rather than a Regulation as this already provides sufficient flexibility under the current framework.

In this context, the UK's Information Commissioner, Christopher Graham warned that an over-prescriptive regulation would be counter-productive. He stressed that there would be a danger of creating something that cannot be done and therefore will be of less use than the current regime. He also emphasised the need for global solutions in data protection regulation, agreeing that modernisation was essential, but highlighted the need to *"engage with partners all around the world".*

EU ministers have yet to agree on the "one stop shop" principle. It seems likely that this will be diluted so that a data controller will be regulated by the regulator in the EU jurisdiction of its main establishment under the condition that it will have to cooperate and work closely with other regulators. This may limit the current advantage to companies of setting up in more favourable regimes such as the UK and Ireland.

The previous Greek Presidency had set great store in creating the right balance between being realistic on the one hand, and not turning a blind eye to the difficulties on the other. Despite this emphasis on balance, it seems that a more heavy-handed approach to regulation could prevail, since new provisions including the extra-territorial effect, the principle of accountability and the need for policies, procedures, audit and appointing a data protection officer along with data breach notification duties and substantial fines all look very likely to be implemented.

Looking forward to September, the next round of discussions on the risk-based approach and the right to be forgotten will be held in the technical working group called "DAPIX". The Italian Presidency has expressed its wish to reach an agreement on the risk-based approach as well as the question of having a higher standard of data protection for the public sector at national level during the September meeting.

Businesses should keep a close eye on the negotiations and seek to engage on key issues, since several issues could be of crucial importance, particularly to SMEs but also more broadly, with regard to the risk-based approach being applied in relation to the documentation requirements, the responsibility of the controller and the data protection impact assessment.

Looking further ahead, businesses and organisations should act early to take adequate steps before the Regulation is eventually adopted: the current forecast is that the texts will be adopted in 2015, even if the ambitious political aim remains to have it finalized in late 2014. Thomas Zerdick, the Head of Reform at the European Commission's Data Protection Unit, confirmed that the Data Protection Regulation is on "*a good track*" for agreement next year.