RegulatoryStrategies

UK Data Protection Newsletter June 2013

Headlines this month:

- ICO 2012/2013 annual report
- Privacy Seal schemes
- Data Profiling
- Guidance on social networking and online forums
- ICO demands more resources
- EU data protection compromise proposal
- Recent data breaches
- EU update

Commentary:

ICO 2012/2013 annual report

The Information Commissioner's Office published its annual report during June. The ICO has stated that the next year will see organisations recognise the need to handle customer data properly - only 10% of organisations understood the legal limitations of how they can use personal information.

Speaking at the launch of the annual report, Christopher Graham, the Information Commissioner said:

"Education and empowerment have been two of the key areas we've focused on in the past twelve months. That work is having real benefits: consumers' awareness of their rights remains strong, and that is empowering people to demand more in return for their data.

The result is consumers expecting organisations to handle their personal data in a proper way, and a legal way. Businesses that don't meet that basic requirement are going to quickly find themselves losing customers.

I think 2013 is the year that organisations will realise the commercial imperative of properly handling customer data. The stats we've seen about public concern around personal data show that, as does a company the size of Microsoft choosing privacy as a theme of a national advertising campaign.

The message to businesses is simple: consumers understand the value of their personal data, and they expect you to too".

The annual report summarises the impact of its **enforcement action** emphasising that, while this is only part of what they do, it is important that the regulator has power to act. Civil penalties of over £2.5 million were imposed on over 23 data controllers for breaches of both the Data Protection Act and the Privacy and Electronic Communication Regulations.

The ICO clearly continues to see its role in **education** as extremely important for data controllers and individuals. It also highlights concerns about future **funding** as the future Regulation (likely to be implemented in 2016) will limit the ICO's discretion in enforcing the law.

The annual report summarises ICO key activities in the last year. In relation to data protection these were:

April 2012
- Guidance published to help individuals delete personal data securely from old devices after finding that one in ten second hand hard drives hold residual personal information.

June 2012
- A guide was launched to offer help to SMEs to make IT systems safe.

July 2012
- Enforcement action taken against Southampton City Council to prevent mandatory recording of conversations in the city's taxis.

August 2012
- Prosecution of a Lancashire bar owner for failing to register use of CCTV equipment.

September 2012
- Guidance published for companies using cloud computing providers.
- Evidence given to the Justice Select Committee on proposed EU data protection proposals.

November 2012
- Launch of the 'Anonymisation code of practice'.
- Two monetary penalties under PECR equating to £440,000 for spam texts.

December 2012
- Launch of a consultation on the 'Subject Access Code of Practice'.
- Bank employee prosecuted under S55 of the Data Protection Act.

January 2013
- Sony Computer Entertainment Europe Limited issued with a £250,000 penalty.
- Response to the Leveson Report published.

March 2013
- A monetary penalty of £90,000 was issued against a company making unwanted marketing calls.
- Guidance issued for organisations allowing staff to use personal devices.

Data protection complaints

The report summarises the volume of data protection complaints handled in 2012/13 showing a **6.3% increase** over the previous years. The ICO handled **13,802** complaints of broken down into the following sectors:

Lenders	17%
Local government	11%
Health	9%
General business	9%
Central government	6%
Policing and criminal records	5%
Telecoms	4%
Education	4%
Insurance	3%
Internet	2%
Retail	2%

Privacy and Electronic Communications Regulations (PECR) complaints

The report shows a **decrease of 10%** in PECR complaints totalling 6,386 in 2012/2013. 49% of the complaints received related to direct marketing and only 9% of the total complaints resulted in enforcement action being considered. The majority of complaints (48%) related to telesales calls where a recorded voice was heard.

Concerns raised about cookies decreased throughout the year - 258 concerns were raised in Q1 compared with only 87 in Q4.

Privacy Seal schemes

The ICO has asked organisations if they would be interested in running an accredited privacy seal scheme to work with them indicating that privacy seals may be introduced in the not too distant future.

Privacy seals feature in the EU draft data protection regulations so, in all likelihood, would have been introduced anyway with the implementation of the new regulation.

Data Profiling

The Article 29 Working Party has produced an advice paper including its suggestions for the new data protection law around data profiling. It attempts to offer 'middle ground' between the EU's current proposal for regulation and the European Parliament's proposals.

Eduardo Ustaran of Field Fisher Waterhouse commented:

"The most challenging aspect of the Working Party's advice is their call for explicit consent and data minimisation. These would be real practical challenges given the omnipresent and evolving nature of profiling and I wonder whether they are fully justifiable from a public policy perspective"

The Working Party has proposed the following definition of profiling:

""Profiling' means any form of automated processing of personal data , intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements."

The Working Party recommends:

- A comprehensive approach to determine specific legal requirements not only for usage and further processing of personal data but for the collection of data for the collection of data for the purpose of profiling and the creation of profiles.
- Mitigation of risk by greater transparency and more individual control on whether or not personal data may be processed for the purpose of profiling.
- Data subjects should have the right to access, modify or delete profile information attributed to them and refuse any measure or decision based on it or have the decision reconsidered through human intervention.
- A higher degree of responsibility and accountability with regard to the use of profiling techniques. Safeguards should include anonymisation or pseudonoymisation.
- There should be a balance between assessing the interests of controllers and the interests, rights or freedoms of data subjects.

Guidance on social networking and online forums

The ICO has issued guidance on social networking and online forums and when the Data Protection Act becomes applicable. The guidance explains what organisations and individuals processing personal data need to consider when running, contributing to or downloading personal data from online forums such as social networking sites, message boards or blogs.

The Data Protection Act includes an exemption for personal data processed for the purposes of personal family or household affairs often referred to as 'domestic purposes'. This exemption does not cover organisational use of online forums and these are therefore subject to the Act and the guidance recognises that businesses, charities and political parties are increasingly using online forums for their ordinary corporate or organisational purposes.

The ICO would expect an organisation running a social networking site or online forum to have policies in place to deal with:

- Complaints from people believing their personal data may have been processed unfairly or unlawfully because they have been the subject of derogatory, threatening or abusive online postings by third parties.
- Disputes between individuals about the factual accuracy of posts.
- Complaints about how the organisation running the site processes any personal data (such has contact details) given to it by its users or subscribers

ICO demands more resources

Christopher Graham, the Information Commissioner, has stated that the draft EU data protection regulation would impose so many new tasks on the regulator that it would not be able to cope with current funding or, with less income, should the current income from notifications be removed.

Graham has written a letter to the Secretary of State for Justice, Chris Grayling, saying that the consistency mechanism which would rely on just one lead Data Protection Authority for multinational companies, would bring more work to the ICO because many regional headquarters are UK-based.

The following areas were highlighted as areas that could bring a negative impact:

- More emphasis on enforcement and fewer resources for education.
- Mandatory data breach reporting for all incidents and not only those posing a significant risk.
- Prior authorisation for international data transfers.
- Limited discretion with regard to fines.
- The consistency mechanism being insufficiently risk-based.

Graham feels that if the ICO does not receive increased funding it will need to change its approach from an educational and advisory one where enforcement occurs where it sees most risks to a process-driven model with prior checking, administering of fines and processing breach notifications

EU data protection compromise proposal

The Council of the European Union has suggested a compromise with regard to the proposed Regulation taking a more risk-based approach. The proposal comes because the Council is keen to see progress with the draft regulation.

The Council wants to limit the scope of the Regulation saying that it should only apply to non-EU controllers if it is clear that the controller is envisaging doing business with data subjects residing in more than one Member State.

The Irish presidency is proposing that direct marketing would be included in the grounds for processing based on legitimate interests and suggests the consent requirement be changed from "explicit" to "unambiguous".

The Council is also suggesting an amendment to the 'household exemption': 'Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities'.

Viviane Reding, Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, has said that she will not accept a level of protection lower than in the current EU data protection Directive on any particular issue. Reding is keen to retain "explicit" consent and data minimisation in the draft.

Recent data protection breaches

Nationwide Energy Services / We Claim You Gain

The Information Commissioner's Office has issued two monetary penalties amounting to £225,000 to Nationwide Energy Services and We Claim You Gain - both companies are part of Save Britain Money Limited and have been involved in the BBC programme 'The Call Centre'.

One penalty is the first to be issued against a company involved in 'nuisance calls' relating to Payment Protection Insurance.

The penalties were found to be responsible for over 2,700 complaints to the Telephone Preference Service (TPS) and to the ICO. It was found that inadequate checks had been made to determine whether the people called had registered with the TPS contravening the legal requirement placed on organisations under the Privacy and Electronic Communications Regulations.

The ICO has welcomed discussions in the House of Commons about how the law can be improved to prevent unwanted marketing calls and texts. It believes more can be done to address this and the ICO continues to offer an on-line tool for individuals to report unwanted marketing. The ICO currently has 10 further investigations underway.

North Staffordshire Combined Healthcare NHS Trust

A penalty of £55,000 was issued to North Staffordshire Combined Healthcare NHS Trust further to sensitive medical details relating to three patients being sent to a member of the public. The fax number was incorrectly dialled each time.

Procedures existed to make sure that staff would make calls prior to sending faxes to ensure that they were sent to the correct address but these had not been communicated to staff.

Glasgow City Council

A monetary penalty of £150,000 has been imposed on Glasgow City Council further to the loss of two unencrypted laptops containing the details of over 20,000 people. The council had been issued with an enforcement notice three years ago following the loss of an unencrypted memory stick containing personal information. Despite the previous incident, unencrypted laptops had been issued and 74 unencrypted laptops were now accounted for. An ICO spokesperson commented:

"How an organisation can fail to notice that 74 unencrypted laptops have gone missing beggars belief. The fact that these laptops have never been recovered,

and no record was made of the information stored on them, means that we will probably never know the true extent of this breach, or how many people's details have been compromised."

A further enforcement notice has been served on the council requiring a full audit of its IT assets, training of

Halton Borough Council

A penalty of £70,000 was issued to Halton Borough Council further to a council employee sending a letter about an adopted child to the birth mother and including a letter in error giving the adoptive parents home address. The child's birth grandparents subsequently wrote to the address seeking contact with the child.

The ICO found that there was not a clear policy and process for checking correspondence.

Stockport Primary Care Trust

A £100,000 penalty was issued to Stockport Primary Care Trust after a large number of patients' details were found at a site previously owned by the Trust. The details were found by the subsequent owner as part of boxes of waste including diaries, letters, referral forms and patient records including sensitive information.

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:

This month, data protection has dominated the headlines as **concerns erupted over the controversial PRISM system which allows the US National Security Agency (NSA) to gain access to the private communications of users of Internet services,** such as Microsoft, Yahoo, Google, Facebook and Skype. European Commission Vice-President Viviane Reding, responsible for justice, fundamental rights and citizenship, described this as a 'wake up' call that showed how urgent it is to proceed with the EU's data protection package.

Viviane Reding and her EU Commissioner colleague Cecilia Malmström, responsible for home affairs, both have praised the Irish Presidency for the good work done in the Council this year, with the Presidency having submitted a provisional text of the first four chapters to the Council, composed of the 27 Member States. Following a debate between Justice Ministers on 6 June, Irish Minister Alan Shatter announced that a consensus had been reached on the concept of risk-based approach, which should make the legislation more business-focused and pragmatic.

Significant emphasis is also being placed on the principle of proportionality and on other fundamental rights, including the freedom to conduct a business.

In other changes, the Council proposes the introduction of a new category of **pseudonymised data**, which is personal data processed in a way that cannot be attributed to a specific data subject without the use of additional information. It is also proposing to remove the requirement for the data controllers to provide fair processing notices where the data are collected from publicly available sources, which would demand far less resources from companies in terms of compliance than foreseen in relation to the Commission's original proposal.

A number of other issues which will affect the overall burden of the legislation on companies remain open, where one or more Member States are still seeking more satisfactory results.

For example, the UK and the Netherlands criticised the costs the reform will create for SMEs. France, Italy and Greece called for the insertion of a clause asking for the explicit consent of individuals to the treatment of their data by public or private companies.

On the issue of PRISM, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) held an exchange of views with Viviane Reding on 19 June, who commented that the data protection proposal has an important part in helping to resolve the legal uncertainties for the companies collecting and handling personal data of Europeans. The MEPs were scathing in their criticism of the US surveillance system and the implications for the protection of data relating to EU citizens and demanded that the Commission restore a clause - once considered and then dropped – which would create a legal framework on transfer of data to third countries, while the Commissioner claimed this was unnecessary and already covered in the draft Regulation.

With tri-party negotiations expected to begin between the Commission, Parliament and Council over the coming months, some of the main battles are expected over data transfers to third parties in the light of the PRISM affair, and on the question of using anonymised and pseudonymised data when processing. The incoming Lithuanian Presidency, starting in July and which will lead negotiations on behalf of the Council, has admitted that the situation is difficult and the Lithuanian Ambassador to the EU H.E. Raimundas Karoblis said recently that while the Irish have made some progress, it is not enough for breakthroughs. He added that it is necessary to work on the document, but the package is too big and also has too many interconnections with the Directive on passenger name records.

The latest indications from the Parliament's Rapporteur, Jan Philipp Albrecht MEP, are that the responsible Parliamentary Committee LIBE will vote sometime between mid-September and mid-October, after which the tri-party negotiations should begin. There are still key opportunities for companies to influence the process by setting out their positions to the key players over the coming weeks.

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