RegulatoryStrategies

UK Data Protection Newsletter October 2015

Headlines this month:

- Safe Harbor changes
- EU Commissioner – protection of data
- Changes to leadership at the ICO
- Cross-border privacy enforcement
- High profile data security incidents
- Other recent data protection breaches
- EU update

Commentary:

Safe Harbor changes

Department of Culture Media and Sport

The European Court of Justice (ECJ) ruled that Safe Harbor - a pact between the US and the EU that has been in place for 15 years - was invalid in the 6th October. The Information Commissioner's Office has commented further about the concern and interest this has caused. Safe Harbor has been used to give businesses the assurance that, should they transfer date to the US from the EU, that data would be adequately protected therefore helping to ensure that obligations under the 8th Data Protection Principle were met.

The Deputy Commissioner, David Smith, commented:

"The judgment did not strike down Safe Harbor itself, but focused on the Commission Decision that had given assurances to businesses. That means there is still a measure of protection for personal data transferred under the scheme – the privacy principles that members sign up to are still positive, for instance. But the assurance that meant Safe Harbor was automatically considered to provide the adequate protection required under the 8th Data Protection Principle is no longer there."

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

The 8th Principle states:

"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

The ICO has issued advice to businesses as follows:

- **Don't panic:** Businesses should not rush to adopt alternative methods to Safe Harbor which may be less effective. Transfers may always be made on the basis of individual consent but this does not necessarily protect data any more than Safe Harbor – Safe Harbor does give some protection even though it may not be perfect.
- **Take stock:** Businesses should assess exactly what information is being transferred outside the EU and the arrangements in place to ensure it is protected. They should decide whether the arrangements are the most appropriate following ICO guidance. The advice is not to change rapidly and a new, safer and rebranded Safe Harbor may emerge.
- **Make your own mind up:** UK businesses do not have to rely on Commission decisions on adequacy – UK law allows businesses to make their own adequacy assessments.

The ICO has made clear that it will not rush to use enforcement powers. The ICO will be pushing for a new, updated version of Safe Harbor and will be relying on UK law to make any assessments. However, some reports state that January 2016 is muted as the point at which supervisory authorities may begin to take enforcement action.

The ICO's guidance on Assessing Adequacy for International Data Transfers is summarised below:

- **The nature of personal data:** The nature of some data transfers may pose little risk to individuals but clearly a transfer of eg sensitive personal data will be a much higher risk.
- **The purposes for processing:** Data being processed for internal company or group purposes will place far less of a risk than customer contact data.
- **The period of processing:** It may be that some data will be processed only once or for a limited period of time. One-off transfers may be far less of a risk that regular transfers.
- **The country or territory of origin:** Where data originates from outside the EEA it may be that the same levels of security have not been met while EEA companies should always adhere to the same levels of data protection.
- **The country or territory of final destination:** The level of protection in the final destination for data transfers should be assessed.
- **Security measures in the country or territory of destination:** Technical measures may be deployed to help protect data eg encryption / information security standards.

Businesses should also conduct a legal adequacy assessment where an operation or large data transfers are being sent to a third country. Consideration should be given to:

- Is there a data protection regime in place meeting Article 29 Working Party standards?
- Is there a legal framework for the protection of the rights of individuals?
- Does the country recognise the general rule of law?

A statement made by the Article 29 Working Party says:

"The Working Party is urgently calling on the Member States and the European Institutions to open discussions with the US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights. Such solutions could be found through the negotiations of an intergovernmental agreement providing stronger guarantees to EU data subjects. In any case, these solutions should always be assisted by clear and binding mechanisms and include at least obligations on the necessary oversight of access by public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights."

EU Commissioner – protection of personal data

EU Commissioner, Vera Jourova, has stated that personal data protection is a fundamental right and applies when data is sent to third countries saying "Europe is not – and never will be – a 'digital' island".

She stated that two thirds of EU internet users do not trust it and that 42% worry that online payments are not safe – this was why the data protection reform was launched.

She continued that the new Data Protection Regulation:

"... will strengthen and better protect people's fundamental rights and freedoms ... will also restore trust in the internet and the Digital Single Market ... will simplify companies' legal environment ... will create a level playing field for all companies offering goods or services online and by doing so, will boost the European digital economy ... European data protection authorities will have more power to uphold the fundamental right to data protection".

Changes to leadership at the ICO

The Information Commissioner is to be assisted by a Senior Management Team of 12 colleagues from November. Deputy Commissioner David Smith is to retire after 25 years at the ICO.

Christopher Smith commented:

"At the end of June 2016, I will have done my seven years as Information Commissioner ... the advertisement for my successor will be published shortly.

"The next Information Commissioner will have the challenge of leading the ICO through an exciting period of change as the organisation gears up to apply the new DP Regulation. Add that dimension to what is the roller coaster ride that upholding information rights in the digital age involves ..."

Cross-border privacy enforcement

The ICO has signed an agreement to be involved in a technical solution for international agencies involved in privacy enforcement called the GPEN alert – Global Privacy Enforcement Network.

The Information Commissioner commented:

"It is clear that organisations' use of data is getting more complicated, and ever more international.

"People need to know privacy authorities around the globe are watching over their information, and that policing of the rules doesn't stop at a country's border.

"The launch of the GPEN alert today is an important step in achieving that, building on the international cooperation the GPEN network has developed. By providing a secure and confidential system, we hope it will provide a key tool in the future."

High profile data security incidents

The ICO has made a statement in light of the recent Talk Talk data security incident:

"Any time personal data is lost there can be a risk of identity theft. There are measures you can take to guard against identity theft, for instance being vigilant around items on your credit card statements or checking your credit ratings".

Talk Talk were subject to a security attach on 21st October. Police have arrested and bailed a 15 year old boy from Northern Ireland, a 16 year old boy from West London and a 20 year old man from Staffordshire in connection with the cyber attach,

Talk Talk's Chief Executive Officer has said that the attached was "much smaller than originally suspected." Although it has been said that up to 28,000 obscured credit and debit cards and 15,000 dates of birth had been accessed by hackers.

This is the third of three separate cyber attached affecting Talk Talk in the last year. Talk Talk were criticised by the Information Commissioner's Office for taking more than 24 hours to notify them of the breach.

October also saw Experian in the US hacked where 15 million individuals were put at risk including T-mobile customers. US privacy groups have called for a Federal investigation.

Vodafone has stated that hackers may have accessed bank details of 2,000 customers and has notified the National Crime Agency, Ofcom and the Information Commissioner's Office.

The Royal Bank of Scotland has been accused of 'falsifying' customer information by editing customer emails and call recordings. RBS are complying with the ICO.

Other recent data protection breaches

Help Direct Limited

Help Direct Limited has been fined £200,000 by the ICO for sending out thousands of unsolicited marketing text messages. Help Direct is a lead generation company.

A marketing campaign generated 6,758 complaints in one month. The messages included offering services such as PPI reclaim, accident compensation claims, bank refunds and loans.

The ICO also issued an enforcement notice to Help Direct earlier in the year ordering them to stop sending marketing texts.

The ICO commented:

"This was a marketing campaign on a massive scale from a company who has already been warned by us to stop sending these marketing messages.

"Help Direct has deliberately broken the law by continuing to send these messages, which is why the company has received the first monetary penalty under our new powers".

Pharmacy 2U

Pharmacy 2U is an online pharmacy which has been fined £130,000 for selling details of over 20,000 customers to marketing companies. Companies buying the details included a health supplements company which had been cautioned for misleading advertising and an Australian lottery company under investigation by Trading Standards. The company had not advised its customer that it intended to sell their details.

David Smith, the Deputy Commissioner, said:

"Patient confidentiality is drummed into pharmacists. It is inconceivable that a business in this sector could believe these actions were acceptable. Put simply, a reputable company has made a serious error of judgment, and today faces the consequences of that. It should send out a clear message to other companies that the customer data they hold is not theirs to do with as they wish."

Anglesey County Council

Anglesey County Council has been ordered to improve data protection practices – two separate security incidents led them to signing undertaking to make changes but audit visits still found unresolved problems. An enforcement notice has placed an obligation on the Council to introduce mandatory training for staff, maintain a records management policy and ensure appropriate controls are in place when staff leave the organisation.

EU update

RegulatoryStrategies

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:

Negotiations on the EU General Data Protection Regulation (GDPR) are now on track, with a potential deal in sight by the end of this year. The latest inter-institutional trialogue meeting, which took place in the last days of September, saw Council representatives and the European Parliament's negotiating team debating the principles for protecting personal data (Chapter II), the rights of the data subject (Chapter III) as well as the rights and duties of data controllers and processors (Chapter IV).

Briefing the European Parliament's Justice and Home Affairs Committee, the German MEP leading the negotiations, Jan Philipp Albrecht, affirmed that a political agreement had been reached on about 70-80% of the chapters mentioned above. The remaining open issues - such as the form and conditions for individuals to give consent to the processing of personal data; the principles and definitions of data minimalisation; the duties to inform in a transparent manner as well as the duties for controllers and processors – should be revised by November by the two institutions' technical advisers. Mr Albrecht also informed the Committee about the agenda of the fourth trialogue meeting which would focus on the role of independent supervisory authorities (chapter VI) and law enforcement (chapter VII). In his concluding remarks, the German MEP said he was optimistic about the prospects of reaching a final compromise on the GDPR with the Council by the end of 2015.

On the Council side, on 9 October, EU Justice Ministers agreed their negotiating stance on the draft Data Protection Directive for police and criminal justice authorities which, together with the GDPR, represents the core of the legislative package adopted in 2012 by the European Commission to reform the EU data protection legal framework. The Directive aims at protecting personal data processed for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences or the safeguarding against and the prevention of threats to public security. Its objective is to ensure a high level of protection of personal data and to facilitate the exchange of personal data between law enforcement authorities within the EU. The agreement within the Council was welcomed by the European Commission and the European Parliament which wants to include the two pieces of legislation in one single package when coming to negotiations in order to increase its political leverage.

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

The current European data protection framework experienced a major evolution in early October. Taking into account the opinion of one of its Advocate Generals in September, the European Court of Justice (ECJ) declared on 6 October that the EU-US data sharing agreement known as 'Safe Harbour' was invalid and criticised the US government for "compromising the essence of the fundamental right to respect for private life". The ECJ ruled the agreement illegal on the basis of the inadequate protection given to Europeans' data once it is transferred to the US. The concept of 'Safe Harbour' allows companies to transfer consumers' personal data from Europe to the US if they vouch for adequate privacy standards. According to the ECJ, the regime undermined the ability of national data protection authorities to determine whether data transfers to the US had privacy safeguards in line with EU legal standards. In an effort to reassure companies, the European Commission commented on the ECJ ruling by stating that they "will continue their work towards a renewed and safe framework for the transfer of personal data across the Atlantic", while "in the meantime, transatlantic data flows between companies can continue using other mechanisms for international transfers of personal data available under EU data protection law".

In terms of next steps, EU institutions are confident that negotiations on the GDPR will be concluded by December 2015, which still gives businesses the opportunity to pursue lobbying activities to influence the EU decision-making 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