Bird & Bird & data protection update

November 2013

We are enclosing our latest data protection update of news and developments in October.

Key points to note are as follows:

- The European Parliament LIBE committee voted for the package of a new Regulation and a separate Directive on data protection for law enforcement purposes.
- The Ministry of Justice was fined for accidentally releasing sensitive information of prisoners to members of the public.
- The First Tier Tribunal has overturned a monetary penalty issued for text marketing in breach of the Privacy and Electronic Communications (EC Directive) Regulations 2003, on the basis that spam texts may be a nuisance but do not cause substantial damage and distress.
- European Data Protection Authorities discuss a wide range of issues, including: cookies, PRISM and Passenger Name Records.

As ever, please do not hesitate to contact us if you have any queries.

Ruth Boardman
Partner
ruth.boardman@twobirds.com

Title	Description
UK	
Information Commissioner's Office (ICO)	
03 October 2013	**ICO seeks feedback on privacy notices code of practice** The ICO is reviewing its privacy notices code of practice. The Code, which was first published in June 2009, is designed to assist organisations with the collection and use of personal data in accordance with the first principle under the DPA. The ICO is seeking feedback on how the Code could be improved by 22 November 2013. **The existing code of practice can be found here.**
09 October 2013	**Information Commissioner briefs Home Affairs Select Committee on PI investigation** The Information Commissioner, Christopher Graham, has briefed the Home Affairs Select Committee regarding the ICO's investigation into possible breaches of the DPA by clients of a group of rogue private investigators. In his letter of 30 September, the Commissioner confirms that evidence examined between 2001 and 2009 links 19 clients from a number of sectors, including the security, financial, construction, general retail and legal industries, to data protection breaches. The ICO investigation is anticipated to be complete in eight months. **The ICO news release can be read here.**
10 October 2013	**Government to consult on introduction of custodial penalties for data protection breaches** The Lord Chancellor, Chris Grayling, has confirmed in a letter to Home Affairs Committee, plans by the Government to consult on the introduction of custodial penalties for breaches of section 55 of the DPA. Under section 55 DPA, the knowing or reckless obtaining or disclosure of personal data without the consent of the data controller is an offence, as is selling or offering to sell data so obtained or disclosed. The proposed custodial penalties could last up to 12 months on summary conviction and two years imprisonment for a conviction on indictment. The announcement follows the Home Affair Committee's inquiry into the role of private investigators as part of the phone-hacking scandal. The move has been welcomed by the ICO. **A full summary of the Government's plans can be found here.** **The Lord Chancellor's letter can be found here.**

15 October 2013

ICO warns organisations of BYOD risks following Royal Veterinary College data breach

The ICO has warned organisations to ensure that their data protection policies adequately reflect the growing trend of Bring Your Own Devices (BYOD) after the Royal Veterinary College found that a memory card from the camera of a member of staff containing the passport images of six job applicants was stolen.

The ICO's guidance outlines the key issues organisations should be aware of when staff take advantage of BYOD, including:

- Being clear with staff about which types of personal data may be processed on personal devices and which may not;
- Using a strong password to secure the devices;
- Enabling encryption to store data on the device securely;
- Ensuring that access to the device is locked or data automatically deleted if an incorrect password is inputted too many times;
- Treating all public cloud-based sharing and public backup services, which have not been fully assessed by organisation, with extreme caution;
- Registering devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft.

The ICO news release can be read here.

The ICO BYOD guidance can be accessed here.

22 October 2013

ICO and Ofcom announce international effort against telephone caller identification spoofing

Ofcom and the ICO have announced a collaborative effort with agencies in Canada and the US to combat telephone caller identification spoofing. This type of spoofing, where callers use technology to hide their caller ID with inaccurate, false or misleading information, is a breach of the Privacy and Electronic Communications Regulations 2003. It is hoped that the collaboration will assist each of the respective countries to uncover a solution which will enable the agencies "to put a stop to this harmful practice and take action against those responsible".

The ICO statement can be found here.

Title	Description
UK	
Cases	
***Niebel v Information Commissioner* (2013)** **First-Tier Tribunal General Regulatory Chamber** **Information Rights** **EA/2012/0260** **14 October 2013**	**Full judgment released as penalty notice is cancelled** The appeal was made by Mr Niebel of Tetrus Telecoms in respect of a monetary penalty notice (the "**notice**") issued on 26 November 2012 requiring him to pay £300,000. The Tribunal considered evidence which showed that Mr Niebel had been sending unwanted text messages on an "industrial scale" from unregistered SIM cards, seeking out potential claims for mis-selling of PPI loans or for accidents. This was in clear breach of regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**") relating to the sending of text messages for direct marketing purposes on a prior consent basis. Since 26 May 2011, the ICO's power to impose monetary penalties has been subject to certain preconditions: firstly it must, inter alia, be a serious offence; and secondly, it must be "of a kind likely to cause substantial damage or substantial distress". The penalty was calculated by reference to 732 texts (i.e. the number of text messages allegedly sent from 26 May 2011). However, parts of the notice appeared to refer to a contravention on a much wider scale. Following the notice, the ICO discovered that only 286 texts were actually sent after 26 May 2011. The appeal centred around one core issue: was the contravention caused by sending only 286 texts was not of a kind likely to cause substantial damage or distress? Mr NJ Warren held that by looking at the narrower range of evidence available, the contravention thresholds were not satisfied on the basis that by only sending 286 texts between 26 May 2011 and 9 November 2011, there was no "substantial" damage or distress caused. From a damage perspective, the Tribunal determined that despite the fact that recipients would have incurred charges by replying "stop" to the texts or by receiving texts abroad, these charges would have more likely caused "irritation" to recipients rather than "substantial damage". Furthermore, "substantial distress" was unlikely on the basis that, according to the Tribunal's reasoning, "almost all mobile phone users…will recognise these texts for what they are". The Tribunal allowed the appeal and cancelled the notice. Due to the procedural difficulties which beset this case, it is still uncertain as to how many unwanted marketing texts would need to be sent to give rise to substantial damage or distress. The decision will be of importance in respect of future appeals about monetary penalty notices under the PECR. **The full judgment may be read here.**

Title	Description
UK	
Enforcement	
04 October – 31 October 2013: Four undertakings, one prosecution and two monetary penalty notices.	The enforcement period for this month includes: a number of undertakings by four public authorities in respect of the loss of sensitive personal data, an undertaking for Panasonic UK for data loss following the theft of a laptop; the prosecution of a pay day loan company for failing to register with the ICO; and a monetary penalty notice against the Ministry of Justice for accidentally releasing prisoner details to the members of the public. **Please see attached Enforcement Table for more details.**

Title	Description
Europe	

EU Data Protection Reform

07 October 2013

Council ministers likely to reach an agreement on the "one-stop shop" mechanism

In addressing the Justice Council, Viviane Reding, Vice-President of the European Commission, and EU Commissioner for Justice, called for unanimous support for the "one-stop shop" mechanism outlined in the draft Data Protection Regulation.

Reding explained the positive aims of the mechanism as follows:

- Businesses will have one interlocutor,
- Individuals will always have the protection of their local data protection authority including in transnational cases, and
- Data protection authorities will be strengthened by working together to deliver better and more consistent protection throughout the Union.

Reding went on to explain that for "one-stop shop" to work, there needs to be a balance between the role of the authority of the main establishment, and the powers of the authority which receives a complaint. This is to be achieved by:

- The authority of the main establishment retaining meaningful powers; and
- An increased role for data protection authorities in order to guarantee the proximity of decision-making to citizens, for example by having the power to escalate discussions to the European Data Protection Board.

A final decision is to be made by the Council of Ministers in December.

The full press release on the "one-stop shop" mechanism can be found here.

21 October 2013	**LIBE vote on draft data protection Regulation and separate Directive** The LIBE committee voted for the package of a new Regulation and a separate Directive for the law enforcement sector; on the back of a revised text of amendments. The overall aim now is to adopt the new legal package before the end of the current legislature. This vote gives a mandate to the Rapporteurs, MEPs Albrecht and Droutsas, to negotiate with the Council of the EU. On 7 October 2013 Ministers in the Council discussed the data protection reform and reached an agreement in principle on the "one-stop shop" mechanism. The next meeting of Justice Ministers on the data protection reform will take place on 5-6 December 2013. **The Bird & Bird news alert can be found here.** **The Article 29 Working Party press release can be read here.** **The European Commission press release can be read here.**

Title	Description
Europe	
Article 29 Working Party	
09 October 2013	**European Data Protection Authorities discuss cookies, PRISM, Microsoft, and Passenger Name Records** **Cookies** The A29 WP adopted a working document providing guidance on obtaining consent for cookies. The Opinion sets out what organisations must do to comply with laws of all Member States; namely: • The information provided must be specific and appropriate • Consent must be sought before the processing starts, so before (non-functional) cookies are set • Consent must be unambiguously and freely given, which means that there should be no doubt that the data subject has given consent. **The Bird & Bird news alert can on the Opinion can be found here.** **Passenger Name Record (PNR) agreement EU - Canada** A letter was sent to the LIBE Committee expressing concerns regarding the proposal for a Council decision on the PNR agreement between the European Union and Canada. Concerns included: • The use of PNR data for law enforcement purposes, as PNR data are generated for commercial purposes and their reliability is not checked. • There is currently no factual evidence demonstrating to what extent the use of the data contributes to public safety; and • The further processing of PNR data can be very intrusive to the data subject.

PRISM

The Working Party is continuing to assess the consequence of PRISM and related programmes on the privacy of the European Union's citizens' personal data.

Other issues

The Working Party met with representatives of the Lithuanian presidency of the Council and from the Council of Europe to discuss the on-going data protection reforms. The Working Party also discussed on-going work on opinions on legitimate interests and device fingerprinting.

The full press release can be found here

The 2013 working document on cookies can be accessed here

The letter sent to the LIBE committee on the PNR agreement can be accessed here.

Title	Description
Europe	
EDPS (European Data Protection Supervisor)	
22 October 2013	**EDPS welcomes LIBE vote on data protection reforms** The EDPS is keen for the proposals outlined in the data protection reform package to be adopted before a new Parliament elected, as this would mean the proposals would have to be re-examined from the beginning. The EDPS also highlighted the importance of the reform in the wake of the Edward Snowden revelations, in that individuals will be able to: • Expect clear information on how their personal data will be used by organisations • Have the right to ask companies to erase their data in circumstances which do not conflict with freedom of expression rights Finally, the EDPS welcomed the one-stop-shop approach for industries, which will enable them to make the complaints process more efficient as well as introduce a level of consistency. **The press release can be read here.**

Enforcement notices and undertakings

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
04 October 2013	Cardiff & Vale University Health Board	**Undertaking**	A consultant psychiatrist lost a bag containing sensitive personal data including a Mental Health Act tribunal report, a solicitor's letter and five CV's whilst cycling home from the office. The individual did not receive induction training on data protection until after the incident had occurred.	**Cardiff & Vale University Health Board to:** • Put in place adequate security policy for the removal of documentation off site and the security of the data whilst in transit. All staff to be made aware of that policy and trained in how to follow it; • Make all data protection training mandatory in relation both the requirements of the Act and the Health Board's policies relating to the use of personal data. Completion of the training to be recorded and monitored to ensure compliance; • Assess staff for their suitability for home working and appropriate arrangements made for the most secure method of transporting the relevant data, where appropriate; • Put in place appropriate protective marking scheme and make use of redaction techniques where possible; and • Ensure that compliance with the Health Board's policies on data protection and IT security issues are appropriates and regularly monitored.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
07 October 2013	Hillingdon Hospitals NHS Foundation Trust	**Undertaking**	Cancer referral forms containing sensitive clinical data were found in the possession of a local newspaper. The forms were prepared for transfer between The Hillingdon Hospital and Mount Vernon Hospital but failed to arrive through the internal mail system. Although staff were aware of the problem they did not escalate the incident.	**Hillingdon Hospitals NHS Foundation Trust to:** • Ensure that appropriate breach reporting mechanisms are implemented, with staff made fully aware of the reporting procedures and requirements; and • Effectively manage an escalation process in the event that sensitive personal data does not arrive at its intended destination.
08 October 2013	First Financial	**Prosecution**	A London-based pay day loans company and its director, Mr Hamed Shabani, were prosecuted by the ICO for failing to register the business with the Information Commissioner. The sole director and shareholder was prosecuted personally.	**Fine of £150 plus £50 victims' surcharge plus £1,010.66 contribution towards prosecution costs.**

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
15 October 2013	Royal Veterinary College	**Undertaking**	A memory card containing passport photos of 6 job applicants was stolen from a camera owned by an employee of the College. As the camera was a personal device it fell outside scope the College's policies and procedures.	**Royal Veterinary College to:** • Ensure that mandatory induction and annual refresher training in the requirements of the DPA is provided to all staff whose role involves the routine processing of personal data by no later than 30 April 2014; • Record and monitor the provision of such training with oversight provided at a senior level against agreed KPIs to ensure completion. The College to implement follow-up procedures to ensure that staff who have not attended or completed training do so as soon as practicable; • Ensure that portable and mobile devices including laptops and other media used to store and transmit personal data are encrypted using encryption software which meets the current standard or equivalent and advice is provided to staff on the use of such media devices by no later than 30 April 2014; and • Ensure that physical security measures are adequate to prevent unauthorised access to personal data.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
18 October 2013	Panasonic UK	**Undertaking**	Theft of an unencrypted laptop containing personal data relating to 970 individuals who had hospitality events organised by Panasonic UK including names, passport details, addresses and contact details.	**Panasonic UK to:** • Put in place adequate contracts and checks to ensure that data controllers are capable of, and are continuing to, comply with the seventh data protection principle; and • Ensure that personal data collected for a specified, valid purpose is not held for longer than is necessary for that purpose.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
22 October 2013	Ministry of Justice	**Monetary Penalty**	Three emails containing sensitive information of all of the inmates serving at HMP Cardiff were accidentally sent to three of the inmates' families between 4 – 2 August 2011. Each email included an attachment containing a spreadsheet including the names, ethnicity, addresses, date of birth, details of physical marks including tattoos, sentence length, release dates and coded details of the offences carried out by all of the prison's 1,182 inmates. Six of the prisoners had sex offence information recorded against them. An internal investigation conducted by the Prison revealed that prior to the 2 August 2011 notification by one of the families, the data controller had not been aware that the unauthorised disclosures had occurred.	**Monetary Penalty of £140,000**

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
29 October 2013	North East Lincolnshire Council	**Monetary Penalty**	A special education needs teacher working for the data controller lost an unencrypted USB memory stick containing the sensitive personal data of 286 children. The memory stick was never recovered. The children were aged between 5 and 16 years and the memory stick held data such as: mental and physical disabilities, specific teaching strategies required for a particular child, date of birth, home address and ' home-life' which included financial matters and family dynamics. The ICO found that the loss of this data was likely to lead to the ill-health of those concerned; either through disclosure or a break in the services they were receiving. The potential damage and distress to data subjects, who were deemed 'vulnerable' and their families, was held to be 'substantial'.	**Monetary Penalty of £80,000**

twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Skanderborg & Stockholm & Warsaw