

Bird & Bird & data protection update

June 2013

We are enclosing our latest update of news and developments in June.

Key points to note are as follows:

- The Article 29 Working Party has discussed limits to profiling activities;
- The EU Presidency discussed the pivotal areas of the General Data Protection Regulation; and
- Ofcom has upheld a complaint relating to breach of privacy in a TV programme; a failure to mask a participant's voice meant he was identifiable – a useful reminder that voice can also be a unique identifier.

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)

10 May 2013

ICO assists police with investigation into spam texts

The ICO has assisted City of London Police with an investigation into spam texts relating to reclaiming pensions. The ICO saw a spike in the number of complaints relating to spam texts and cold calls relating to pensions in the past three months. Following information provided by the ICO and several other agencies, the City of London Police carried out a major investigation into pension liberation fraud. Several arrests were made across the UK after the City of London Police entered offices in the City of London.

The ICO news release can be read [here](#).

Title	Description
UK	

Information Commissioner's Office (ICO)

14 May 2013

Independent report shows lack of understanding of proposed data protection reforms

An ICO-commissioned report based on a survey of 506 businesses highlighted both a lack of understanding of the key proposed provisions being proposed, as well as an inability to quantify and estimate their current and projected data protection expenditure.

In summary:

- 40 per cent of companies don't fully understand any of the ten main provisions being proposed
- 87 per cent unable to estimate likely costs of draft proposals to their business
- 82 per cent of survey respondents were unable to quantify their current spending on data protection
- Estimated average costs of data protection are skewed by a small number of observations by large organisations, who are more able to put a figure on their data protection expenditure
- The vast majority of companies with over 250 employees or processing more than 100,000 records already employ a member of staff focused on data protection compliance, a key part of EU proposals

The news report can be found [here](#), with the full London Economics report available [here](#).

Title	Description
UK	

Cases

Complaint by Mr C

Ofcom upholds complaint of unwarranted infringement of privacy

Fairness and Privacy Cases

This complaint concerned the programme "Panorama: Gambling Nation", first broadcast on 05 November 2012. The complainant, Mr C, had taken part in the programme, and although he was not named and attempts were made to obscure his face, his actual voice remained audible and this rendered him identifiable. Following the programme, Mr C had been identified on a social networking site by a number of people who knew him.

Ofcom Broadcast Bulletin

Ofcom applied Rule 8.1 of Ofcom's Broadcasting Code ('the Code'), which states that any infringement of privacy in programmes must be warranted. Ofcom conducted its review in three stages.

07 May 2013

Decision: Upheld

Firstly, Ofcom considered the subject matter and concluded that the subject of gambling addiction was sensitive. The private nature of the information, coupled with the safeguards assured to keep Mr C anonymous, meant that Mr C had a legitimate expectation of privacy in the circumstances.

Secondly, Rule 8.6 of the Code states that if the broadcast of a programme would infringe the privacy of a person, consent should be obtained before the relevant broadcast is made, unless the infringement of privacy is warranted. Mr C had consented to his contribution being broadcasted, on the basis that his identity would be protected. Ofcom therefore found that Mr C did not consent to the broadcasted version on 05 November 2012, from which he was identified.

Finally, in determining whether the infringement of privacy was warranted, Ofcom concluded that the broadcaster's right to freedom of expression and its right to receive and impart information without interference did not outweigh Mr C's expectation of privacy in relation to the broadcast.

Ofcom found that Mr C's privacy was unwarrantably infringed in the programme as broadcast.

The full case can be found on page 26 of the Ofcom bulletin, found [here](#).

Title	Description
UK	

Enforcement

30 April 2013 – 01 June 2013:

One new undertaking, two follow-up review of previous undertakings and one prosecution

Two follow-up reviews have been conducted by the ICO, relating to undertakings previously given by two separate entities, to give the ICO assurance that they have appropriately complied with the previous undertakings given to the ICO. One undertaking was given in respect of compliance with the seventh data protection principle. There has also been one prosecution under s55 of the Data Protection Act, for unlawfully obtaining sensitive medical data.

Please see attached Enforcement Table for more details of the enforcement actions.

Title	Description
Europe	

Draft Data Protection Regulation and Directive

24 April 2013

EU Presidency comments on the General Data Protection Regulation

The EU Presidency prepared a Note to the Committee of Permanent Representatives (COREPER) discussing "pivotal issues" which require political guidance, such the scope of the Regulation and the requirement for "explicit" consent.

The Annex to the Note proposes specific drafting amendments.

On the data processing principles themselves, the Presidency noted that they were largely the same as those within the 1995 Directive, except a new principle of data security and confidentiality was added.

Regarding consent, the Presidency acknowledged that the proposed definition of consent is beyond that required under the 1995 Data Protection Directive: many delegations view the new requirement for explicit consent as unrealistic and of little value, especially on the Internet.

The Note also focussed on:

- Material scope
- Territorial scope
- Freedom of expression and access to public documents

The Note can be accessed in full [here](#).

Draft Data Protection Regulation and Directive

09 May 2013

Dates proposed for postponed LIBE vote on draft General Data Protection amendments

The EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) was set to vote on the latest amendments for the draft General Data Protection Regulation on 29 May 2013, but this was postponed due to the high volume of amendments.

A LIBE spokesperson confirmed that the vote will be rescheduled to take place before the summer break with three possible meeting dates for the vote:

- 19-20 June 2013
- 27 June 2013
- 8-9 July 2013

More information can be found on the LIBE website, [here](#).

Title	Description
Europe	

Article 29 Working Party

28 May 2013

Working Party discusses clear limits to profiling

The Art 29 WP adopted an advice paper on the proposed Article 20 of the new Regulation.

Comments include:

- WP29 support for a separate definition of profiling, and the application of Art 20 to the creation and use of profiles, rather than just on decisions taken as a result of such profiles.
- A proposal for additional transparency obligations, including rights of access, modification and deletion of profiles for data subjects.
- A suggestion for increased safeguarding requirements for profile data, including data minimisation, anonymisation and pseudonymisation requirements.
- Support for a "balanced approach" that only implements these specific profiling rules where the profiling *significantly affects* the individual's interests, rights or freedoms. The WP29 accepts that *significantly affect* can have a wide meaning, and so it suggests that the European Data Protection Board should be given a mechanism in the Regulation for issuing guidelines on the interpretation of such a provision.

The full document can be found [here](#) with a press release [here](#).

Title	Description
Europe	

EDPS

30 May 2013

EDPS publishes 2012 Annual Report

The European Data Protection Supervisor (EDPS) completed his strategic review, resulting in a strategy for 2013-14.

Highlights includes:

- Greater interaction with data protection officers (DPOs)
- The impact of the new enforcement policy with regard to complying with the proposed Data Protection Regulation
- The creation of a new sector to deal with new information technologies

EDPS priorities going forward include:

- Providing ongoing guidance and training for DPOs
- Focussing on technological developments, especially those connected to the internet
- Increasing the scrutiny of data protection issues in any reforms to the financial sector
- The establishment of clear rules for the use of personal data in the area of eHealth

The full Report can be accessed [here](#).

03 June 2013

EDPS to work closely with EUROPOL on EU law enforcement

Following the Commission proposal for a new legal framework for the EU Agency for Law Enforcement and Training (Europol), the EDPS has stated that robust data protection considerations can strengthen the credibility of investigations into serious crimes in the EU.

Given the increasingly crossborder nature of this work, the EDPS says it is imperative that clearly defined criteria are outlined for transfers of information to third countries and international organisations.

The proposed idea to cross-reference information stored in different databases to check if individuals or groups are suspected of more than one type of crime could be a cause for concern if data protection safeguards are not put in place.

The EDPS is to supervise Europol's compliance with data protection rules. The EDPS welcomes the emphasis placed on a robust supervision of Europol, that an EU Agency should be supervised by an established and independent European supervisory body.

At the same time, it is essential that the supervision of Europol is carried out in close cooperation with national data protection authorities as is the case for the supervision of EU large-scale IT databases such EURODAC, CIS and others.

The full press release can be found [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*)
21 May 2013	News Group Newspapers	Undertaking	<p>A server holding part of the Sun Newspaper's website was attacked in July 2011 and large amounts of personal data relating to the Sun's customers was leaked onto the internet. None of the data was sensitive personal data; some of it was several years old.</p> <p>The server in question had not been used for its intended purpose and News Group Newspapers accepted that it had failed to follow its own internal IT governance policies adequately.</p>	<p>News Group Newspapers undertook to:</p> <ul style="list-style-type: none"> • Ensure that all its staff are aware of its policy for the storage and use of personal data and are appropriately trained in how to follow that policy; • Improve technical security controls to prevent further unauthorised access to personal data via its web servers; • Regularly monitor compliance with data protection and IT security policies; • Implement measures to ensure that any customer data collected as part of its activities is regularly cleared in line with a defined retention and disposal policy; and • Implement additional security measures to ensure that personal data is protected against unauthorised or unlawful processing, loss, destruction or damage. <p>The full undertaking can be found here.</p>

Date	Entity	Enforcement notice, undertaking or monetary penalty?	Description	Summary of steps required (in addition to the usual steps*)
23 May 2013	Paul Hedges	Prosecution	<p>Mr Hedges was the former manager of a council-run leisure centre in Southampton. His prosecution related to his unlawful obtaining of sensitive medical data relating to over 2000 users of the leisure centre.</p> <p>Mr Hedges was intending to use the data for a new business venture. After he was made redundant by the leisure centre, Mr Hedges emailed the information to his personal email account, as he was intending to set up a new fitness company. The information resulted from the Council's Active Options GP referral service, where patients would be referred by their GP or other health professional to attend fitness sessions. The council was made aware of Mr Hedges' actions after users of the leisure centre reported being contacted by Mr Hedges to join his new fitness service.</p>	<p>Mr Hedges was prosecuted at West Hampshire Magistrates court. He was convicted under s55 of the DPA for unlawfully obtaining sensitive medical data.</p> <p>Mr Hedges was fined £3,000 and required to pay £1,376 towards the costs of prosecution. He was also told to pay a £15 victims' surcharge.</p> <p>The ICO News release can be read here.</p>

31 May 2013	Leeds City Council	Follow –up review of undertaking	<p>The ICO conducted a follow-up investigation of Leeds City Council, following an undertaking given on 28 November 2012, to ensure that Leeds City Council had complied with the requirements in the undertaking which it gave in November 2012.</p> <p>The ICO’s review concluded that Leeds City Council had taken the appropriate steps and put plans in place in order to comply with the undertaking, but the planned work needs to be completed before the Council is fully compliant with its previous undertaking.</p>	<p>The ICO concluded that Leeds City Council still needs to:</p> <ul style="list-style-type: none"> • Continue to develop its “Transforming Procurement Programme”, which will incorporate monitoring arrangements into its strengthened and formalised procurement process. Once the Programme is implemented, the Council should monitor its progress to ensure that data protection requirements are met; and • Ensure that scheduled work relating to IT governance training and secure file transfers is completed. <p>The ICO’s report can be read here.</p>
31 May 2013	Prospect	Follow –up review of undertaking	<p>The ICO has conducted a review into whether Prospect had met the requirements of the undertaking which it gave on 8 January 2013. The ICO found that Prospect had taken some steps and put plans in place to comply with the undertaking, but there was further work to be done.</p>	<p>The ICO has recommended that Prospect takes the following actions:</p> <ul style="list-style-type: none"> • Complete its review of its data protection policies as soon as possible and introduce an information security policy as previously recommended; • Provide annual refresher training to its staff; and • Implement the recommendations from its independent data security review. <p>The full report can be accessed here.</p>

03 June 2013	Stockport Primary Care Trust	Monetary Penalty	<p>The data controller was found to have left behind boxes containing confidential and highly sensitive personal data relating to over 200 data subjects at a decommissioned site.</p> <p>The ICO's review concluded that the data controller had failed to take appropriate organisational measures, such as having a decommissioning policy. The ICO also considered that the existing measures did not ensure a high level of security, with the breach likely to cause substantial distress.</p>	<p>A monetary penalty of £100,000 was issued by the ICO.</p> <p>The monetary penalty notice can be read here.</p>
05 June 2013	Halton Borough Council	Monetary Penalty	<p>A clerical officer working in the data controller's administrative service, while sending a letter from the adoptive parents to the birth mother, accidentally included the address of the adoptive parents. This led to the birth mother's parents getting in touch with the adoptive parents, followed by an unsuccessful Court application for the right to direct contact with the child.</p> <p>The ICO report found a serious contravention of section 4 (4) of the Data Protection Act through the data controller's failure to take appropriate organisational measures against the processing of personal data. This was compounded by the fact that the data subjects suffered</p>	<p>A monetary penalty of £70,000 was issued by the ICO.</p> <p>The monetary penalty notice can be accessed here.</p>

substantial distress from the breach, following inappropriate contact from the unauthorised third parties. Furthermore, the ICO took into account the fact that one of the data subjects in question was a vulnerable child.

*The usual steps required of an entity are to give undertakings that:

1. Staff are made aware of the data controller's data protection policy and procedures, and are adequately trained on how to follow these; and
2. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

This briefing gives general information only as at the date of first publication and is not intended to give a comprehensive analysis. It should not be used as a substitute for legal or other professional advice, which should be obtained in specific circumstances.

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

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.