Bird & Bird

International data protection enforcement bulletin - June 2013

Welcome to the June 2013 International data protection enforcement bulletin.

In addition to a review of enforcement action taken in many of the jurisdictions in which Bird & Bird has offices, we are delighted to include a contribution from our latest Bird & Bird office, in Denmark, and welcome the team on board.

Highlights this quarter include:

- China issues draft Rules for the Protection of the Personal Information of Telecommunications and Internet Users;
- Hungary removes its prohibition on the use of sub-processors;
- Spain unveils its approach to cookies; and
- an update on the new data protection legislation in Slovakia.

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

Ruth Boardman

Partner

ruth.boardman@twobirds.com

Laura Acreman

Associate

laura.acreman@twobirds.com

Enforcement tables by country

Czech Republic

Date	Infringing entity	Details of infringement	Sanction(s) imposed
January 2013	Ministry of Labour and Social Affairs (MPSV)	The MPSV issued sCards, electronic social systems cards used for payment and administration of uninsured social security benefits and benefits in the framework of the state employment policy. sCards also serve to identify entitled individuals and benefits recipients. In connection with issuing sCards, in January 2012 MPSV entered into a 12-year agreement for the administration of benefit payments with a private bank, Česká spořitelna, a.s (ČS). According to the DPA, MPSV transfers sensitive data about entitled individuals and benefits recipients to ČS without statutory authorisation.	The case is still pending, with remedial measures anticipated at the end of June. In related administrative proceedings a fine of up to CZK 10,000,000 (approx. €40,000) may be imposed.
January 2013	Czech Post	Czech Post equipped its personnel with GPS trackers, claiming that employees had consented to carrying the devices. At the end of each day, the devices are collected from those personnel and the data contained within them are anonymously sent to a central office where postal routes are analysed.	Measures for remedy were imposed. The Czech Post is set to defend its actions before the administrative court.
February 2013	High Public Prosecutor's Office in Prague	The High Public Prosecutor's Office in Prague used its website to publish data about the salaries of all its employees, together with their names. The data were published in response to a request filed under the Act on Free Access to Information (Act No. 106/1999 Coll.)	A fine of CZK 100,000 (approx. €4,000) was imposed. The decision has not yet been legally enforced.

Denmark

Date	Infringing entity	Details of infringement	Sanction(s) imposed
02 April 2013	Waterfront Communication A/S	The publicly-owned national rail company, DSB, is accused of using 'dirty tricks' when lobbying, e.g. by collecting 'intelligence' on members of Parliament and critical journalists. The communication company used by DSB, Waterfront Communication A/S, is accused of forwarding sensitive health information on one such journalist to DSB, and at the same time exaggerating the nature of the health information supplied and the consequences of the same about the journalist's ability to do their job.	The Danish DPA (Datatilsynet) has requested a police investigation of the matter.

France

Date	Infringing entity	Details of infringement	Sanction(s) imposed
03 January 2013	Syndicat des copropriétaires "Arcades des Champs Elysées"	The CNIL received several complaints from security agents supervising a building of the association of property owners (the Association), concerning the use of CCTV. These complaints underlined that there was a breach of privacy rules as the CCTV camera permanently monitored their activities. The CNIL asked the Association to remove the camera, but the managing agent refused, stating that the permanent monitoring of the security office was necessary and proportionate to ensure the security of the premises. The CNIL noted that the purpose of the processing was not to ensure the safety of the agents during their presence in the security office but to ensure the safety of the occupiers of the building. The CNIL concluded that such purpose could not justify permanent monitoring of the security agents. Monitoring of the security staff was contrary to the purpose of ensuring the safety of the building and was therefore disproportionate.	The CNIL imposed a nominal fine of €1 on the Association and ordered it to stop the monitoring. The CNIL published the decision on its website as well as on the Legifrance website (an official database of laws and case law). The CNIL's decision was also publicised in the press.

Germany

Date	Infringing entity	Details of infringement	Sanction(s) imposed
07 February 2013	Facebook Inc.	In September 2012, the Hamburg Commissioner for Data Protection and Freedom of Information issued an administrative order against Facebook Inc. The order obliged the US-company to change its practice of automatic facial recognition to comply with data protection standards. The company had to ensure the existing biometric profiles of its registered users would only be created and stored with their consent. Additionally, Facebook must inform users in advance of the risks of this practice	The Hamburg Commissioner for Data Protection and Freedom of Information closed the administrative order against Facebook Inc. as Facebook no longer offers automatic facial recognition.
22 April 2013	Facebook Inc. und Facebook Ltd.	The Independent State Centre for Data Protection of Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz* or ULD) wanted to stop Facebook's real name policy by ordering Facebook Inc. (USA) as well as Facebook Ltd. (Ireland) to allow users to sign in to Facebook using a pseudonym and to unblock those user accounts that had been blocked due to the users not using their real name and other information. According to the Privacy Commissioner and Head of the ULD, Thilo Weichert, Facebook's refusal to permit the use of pseudonyms on its platform infringed the German Telemedia Act.	Facebook Inc. and Facebook Ireland Ltd. objected, arguing they could not be forced to follow the ULD's orders before a court's final adjudication. The Administrative Court (Verwaltungsgericht) of Schleswig held that Facebook Inc. and Facebook Ltd. did not have to follow the ULD's orders, finding German data protection laws inapplicable to Facebook's processing of personal data about German individuals (file numbers 8 B 60/12 and 8 B 61/1). The ULD appealed against the decision of the Administrative Court of Schleswig but the Higher Administrative Court of Schleswig (Oberverwaltungsgericht) confirmed the two decisions of the Administrative Court and rejected the ULD's complaint. As a consequence, Facebook can require its users to register with their real name and can block accounts that do not comply with Facebook's real name policy. The decision of the main proceedings is still pending.

Hungary

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
January 2013	Hungarian – English Bilingual High School in Balatonalmádi	The National Authority for Data Protection and Freedom of Information ("Authority") commenced proceedings as a result of press coverage on the collection of information about the political views of students and teachers. According to the press, students and teachers of the high school were required to inform the principal about: • discussions among the students about recent student demonstrations and/or strikes organised against the reform of the tertiary education system; • whether teachers in any way supported these actions or encouraged students to participate in the demonstrations; and • whether these discussions included questions relating to the limited number of places at universities and the reform of the tertiary education system. The Authority concluded that the high school principal was instructed by the Governmental Agency of Veszprém County (which executes the owner's rights of the high school) to conduct an internal investigation in connection with the accusation that political discussions took place during classes where teachers encouraged students to participate in the demonstrations. Students and teachers were interviewed one by one by the principal. During these interviews names and student class numbers were requested and minutes were taken, although the data subjects were not informed about the purpose of the interviews, nor were they asked to consent to their data being processed. The Authority concluded that the Governmental Agency of Veszprém County was entitled to instruct the high school to conduct an internal investigation. However, the high school should have established detailed rules for the investigation (including the	The Authority ordered the deletion of the personal data collected and imposed a fine of HUF 300,000 (approx. €1,000).

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		rules of data processing). As no framework for the investigation had been established, the high school breached the Privacy Act.	
February 2013	Unknown	The infringing entity offered deposit account contracts together with baby bonds to families and visited them at their homes. According to the complaints received, the representative of the infringing entity was accompanied by a subcontractor. The application forms provided for the bonds and accounts already included the name, place and date of birth of the child, the mother's maiden name, address of the parent and mother's mobile number. Both the representative of the infringing entity and the subcontractor introduced themselves as representatives of a certain credit centre. The National Authority for Data Protection and Freedom of Information ("Authority") investigated: • the credit centre; • the infringing entity, subcontractor and intermediary of the credit centre offering its products; and • the subcontractor of the infringing entity. The Authority concluded that: • it could not be established beyond doubt that the forms were pre-populated with this personal data when the representative of the infringing entity and the subcontractor visited the families; and • the infringing entity unlawfully involved a subcontractor, which enabled the subcontractor to process the personal data without having any legal basis to do so. It was also established that the subcontractor of the infringing entity unlawfully collected and processed personal data and did not inform the data subjects about its activities.	The Authority imposed a fine of HUF 100,000 (approx. €335).

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		The Authority also declared that although the data subject signed the forms and gave their consent to data processing, their consent was not informed.	
February 2013	The Mayor Office of the village of Kisapostag	The data subjects were living in Dunaújváros, but voted during the 2010 municipal elections in Kisapostag in accordance with their official address registration. In order to initiate criminal proceedings regarding suspected forgery of public documents (i.e. giving false data in the address registration form) the mayor requested the notary of Kisapostag to provide him with personal data from the data register. The Authority established that the notary provided the mayor with more information than the mayor was entitled to, thus the notary unlawfully provided personal data in breach of the Hungarian Privacy Act. The Authority also concluded that the personal data concerned was 'special' data (i.e. criminal offence data due to the fact that criminal proceedings were initiated).	The mayor was not entitled to use the data provided by the notary to initiate a criminal proceedings. The Authority imposed a fine of HUF 100,000 (approx. €335).

* Note that the Hungarian DPA usually does not publish the name of the infringing entity.

Italy

Date	Infringing entity	Details of infringement	Sanction(s) imposed
24 January 2013	L'Espresso S.p.A.	The company published articles in the historical online archive of an Italian newspaper (also available through search engines external to the site) containing personal data relating to two claimants and referring to some court cases in which they had been separately involved. The claimants (having been unable to obtain a suitable response from the publisher) asked the company to "remove" those articles or, alternatively, to upgrade and integrate *"the news contained therein, with the necessary clarification of the complete dismissal of any criminal charge... because the crime does not exist"*. The claimants also asked the data controller (a publisher) to adopt measures technically necessary to render all articles inaccessible via common search engines. Following the claim, the publisher adopted the technical measures necessary to prohibit the articles from bring indexed by search engines external to the newspaper's website.	As part of the newspaper's historical online archive, the Garante ordered L'Espresso to prepare a system to report the existence of subsequent developments in the news related to the claimants (for example, on the sidelines of the articles or in the notes) within 90 days of receipt of the decision and to give notice of the fulfillment of that order by the same date
24 January 2013		Casa di Cura Abano Terme Polispecialistica e Termale S.p.A. The entity processed personal data without consent. Although involving just one data subject, the violation consisted of an unlawful communication of particularly sensitive data (relating to the outcome of HIV testing of the claimant) to a person other than the data subject. In its decision of 27 May 2010 the Garante concluded that the company processed the data in violation of Article 26 of the Italian DP Code and Article 5 of the Law no. 135, dated June 5, 1990.	Given the financial position of the company, the Garante issued a fine of €60,000.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		Report no. 14878/67264, dated June 22, 2010 was presented to the company, outlining an administrative violation under Article 162, paragraph 2-bis of the DP Code and informing the company of the right to a reduced fine pursuant to Law no. 689/1981. The company did not take advantage of this option, instead choosing to appeal the decision before the Court of Padua. The Court of Padua, in its judgment dated May 2, 2011, accepted the decision of the Garante and rejected the company's reasons for appeal, based on the *"(...) established illegality of the communication of data relating to direct and indirect diagnostic tests for HIV infection to a person other than the data subject, in the absence of his consent"*.	
24 January 2013	United Music S.r.l.	Data were collected through certain websites (*www.105.net*, *www.radiomontecarlo.net*, www.unitedmusic.it) for profiling purposes. The company ceased this processing activity without notifying the Garante. The Garante issued a notice of violation. The company opposed the Garante's decision, insisting on its position as a single shareholder company, owned by Gruppo Finelco S.p.A. In view of the centralisation of some services dedicated to companies belonging to the Finelco Group and in view of the fact that the legal representative of the two companies had always been the same, it was not deemed necessary to require a new notification to the Garante.	The Garante fined the company €20,000. The Garante applied its discretional criteria in determining the level of such fine taking into account the limited severity of the violation and the positive action taken by the company to remedy the breach.
24 January 2013	Gruppo Finelco S.p.A.	The company processed personal data through a video-surveillance system. In doing so it failed to: (a) inform data subjects; (b) notify the processing to the Garante. In particular, it processed personal data, sent commercial communications, profiled and disclosed that data to third parties; or (c) acquire specific consent to the processing.	The Garante fined the company a total amount of €52,000, broken down as: • €12,000 for violation (a); • €20,000 for violation (b); and • €20,000 for violation (c).

Poland

Date	Infringing entity	Details of infringement	Sanction(s) imposed
24 January 2013 Judgement of the Supreme Administrative Court (I OSK 1827/11)	e-service provider	An e-service provider collected and used personal data (name, personal identification number, position and date of birth) for commercial purposes. This information was not collected directly from the individual but was publicly available, taken from excerpts of the National Register of Entrepreneurs and announcements from the Court and Commercial Journal. The Inspector General of Data Protection (**GIODO**) decided that the e-service provider should have met certain legal obligations (such as providing the individuals with appropriate notice), even though these data were already publicly available. GIODO ordered the e-service provider to inform the individuals concerned in line with Art 25 sec. 1 of the Polish Personal Data Protection Act of 29 August 1997 (**PDPA**) about: • the fact of the data processing; • the controller's full name and address; • the purpose and the scope of the data processing; • from where the data were collected; and • the right to access and correct their data etc.; GIODO requested the e-service provider fulfil the above obligation within 3 months.	The e-service provider filed a complaint to the Voivodship Administrative Court. The Court upheld the GIODO decision and rejected the complaint. The e-service provider brought an appeal to the Supreme Administrative Court. The Supreme Administrative Court overturned the Administrative Court's decision on the basis of procedural mistakes and ordered the case to be reheard. In the Supreme Administrative Court's opinion GIODO should have indicated how to meet the Art. 25 obligations. The Court also noted that meeting the notice obligation would lead the e-service provider to collect more data about those individuals (i.e. their addresses) than had already been collected.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
10 January 2013 Judgement of the Supreme Administrative Court (I OSK 2029/11)	Telecoms Services Provider	A telecoms service provider processed customer personal data having obtained their consent to processing for various purposes. The personal data was processed for several different purposes including marketing activities conducted by the telecoms service provider alone and together with a third party. After conducting an inspection, GIODO ordered the telecoms service provider to ask customers to consent separately for (i) marketing conducted by the telecoms service provider alone and (ii) marketing conducted by telecoms service provider together with a third party.	Upon the company's complaint the Court ruled that GIODO's decision did not infringe the law to the extent that it should be overturned. The company filed an appeal with the Supreme Administrative Court. The Supreme Administrative Court upheld the Court's judgment.
24 January 2013 Judgement of the Voivodship Administrative court (WSA/Wa 1242/12)	The Chief Officer of the Municipal Police	The Municipal Police Chief Officer requested a telecoms service provider disclose a cell phone owner's personal data (i.e. first name, last name and address of a person who was suspected of committing a minor criminal offence). The Chief Officer based his request on Art. 23 sec. 1 point 4 PDPA which states that data processing is allowed *if it is necessary to enforce a right or comply with a legal obligation and to perform legally defined tasks, carried out in the public interest*. The telecoms service provider refused to disclose the requested data, on the basis that it was obliged to keep the requested information confidential under the Polish Telecommunication Law. The Chief Officer filed a motion with GIODO requesting him to oblige the telecoms service provider to disclose the data. GIODO agreed with the Chief Officer and required the telecoms service provider to disclose the requested data.	The telecoms service provider filed a complaint with the Voivodship Administrative Court. The Court found the complaint justified and decided that the Polish Telecommunications Law provided a stronger protection of personal data than the PDPA and the provisions of the Polish Telecommunication Law have priority over PDPA. The Court decided that the Chief Officer could have not based his request on Art. 23 sec. 1.4 of the PDPA. The Court also stated that Art. 23 sec. 1.4 of the PDPA, on which GIODO based its decision, is a very general provision and cannot be used to avoid telecommunications confidentiality. Further, the Court stated that the purpose of such request failed to meet the requirement of necessity and proportionality.
04 February 2013	A sports association	A licensed coach was a member of a sports association and was listed as a coach on the association's website. The individual's licence was suspended. Despite the suspension the individual kept giving lessons.	GIODO ordered the Association to remove the data from its website.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
Judgement of the Voivodship Administrative court (II SA/Wa 1530/12)		On becoming aware of this, the Association announced the suspension on its website. The announcement identified the coach by full name. The coach requested the Association remove his personal data from its website. The Association refused to do so and the coach filed a complaint with GIODO.	The Association filed a motion with GIODO to reconsider its decision, arguing that putting the data on the Association's website was lawful because the Association was processing the data for legally justified administrative purposes. The Association also stated that the coach was a sole trader and his data were publicly available in the register of sole traders. GIODO upheld its first decision and indicated that the data entered to the register of sole traders are protected by the PDPA. The Association filed a complaint to the Court which upheld the decision of GIODO and confirmed that the placement of the coach's personal data on the website was unlawful.
14 February 2013 Judgement of the Supreme Administrative Court (II SA/Wa 2173/12)	Courier Company	A customer of a telecoms service provider ordered a service by phone. The service was to be provided on the terms of an agreement later concluded by the parties. The telecoms service provider prepared the agreement including the customer's personal data. A telecoms service provider employee signed the agreement and couriered it to the customer. The courier who delivered the document verified the customer's personal data by checking his personal ID number and national ID. The customer filed a complaint with GIODO stating that the courier company and the telecoms service provider where unlawfully processing his personal data as it was unnecessary to collect national ID number or the ID card number for the purpose of the service agreement. A GIODO inspection revealed that data were processed based on an agreement which detailed the personal data the courier could process for such purpose. GIODO decided that the courier and the telecoms service provider did not infringe the PDPA.	The customer filed a complaint with the Court. The Court upheld GIODO's decision and rejected the complaint.

Slovakia

Date	Infringing entity	Details of infringement	Sanction(s) imposed
05 February 2013	Legal entity	Infringement of the obligations contained in the Sections 8(2) and 6(1)(i) of the Slovak Data Protection Act which state that: *In the processing of personal data, an identifier of general application (i.e. the birth identification number) may be used for the purposes of identification of a natural person, provided that its use is necessary for achieving the given purpose of the processing.*	A fine of €1,660 was imposed. It was reiterated that data controller must act in accordance with the Slovak Data Protection Act and other general legal regulations. The controller cannot force the data subject's consent.

Spain

Date	Infringing entity	Details of infringement	Sanction(s) imposed
10 January 2013	La Vimetera S.L	A police inspection revealed sixteen surveillance cameras and a monitor in the director's office. Two of the cameras were positioned in offices used as changing rooms and filmed female staff getting changed at work. The recordings had been on-going for ten days without the surveillance file being registered in the company's name.	By virtue of Articles 45.2, 45.4 and 45.5 of LOPD, the SDPA imposed a fine of €50,000 for a breach of Article 4.1 of LOPD (the data quality principle), classified as a serious breach by Article 44.3. c) of the LOPD. By virtue of Articles 45.1, 45.4 and 45.5 of LOPD, the SDPA imposed a fine of €1,100 for breach of Article 26.1 of LOPD (not notifying the SDPA about the creation of a data file), classified as a minor breach by Article 44.2.b) of the LOPD.
10 January 2013	Banco Mare Nostrum SA	The details of two claimants had been put onto a list of defaulters although the claimants had not received a request for outstanding payment.	By virtue of Article 45.5 of LOPD, the SDPA imposed a fine of €20,000 on Banco Mare Nostrum SA for breach of Article 4.3 of LOPD (data must be updated and correct), classified as a serious breach by Article 44.3. c) of the LOPD.
17 January 2013	Asociación Española de Leasing y Renting	It was possible to click on a link in a third party website to access the webpage of the Asociación Española de Leasing y Renting and enter their website without any restriction on access. It was therefore possible to consult the Register of Vehicles and look up number plates, surnames and insurance details of vehicles.	By virtue of Article 45.2 of LOPD, the SDPA imposed a fine of €20,000 on the Asociación Española de Leasing y Renting for breach of Article 9 of LOPD (data must be kept with the necessary security measures), classified as a serious breach by Article 44.3. h) of the LOPD.
18 January 2013	Yves Rocher España	The claimant asked Yves Rocher to remove her data from their system so as not to receive further direct marketing emails. She continued to receive such emails despite receiving confirmation that she would no longer do so.	By virtue of Article 39.1.b) 40 of LSSI, the SDPA imposed a fine of €33,000 on Yves Rocher España for breach of Article 21.1 of LSSI (sending commercial emails without consent) classified as a serious breach by Article 38.3. c) of the LSSI.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
12 February 2013	Cableuropa SAU	The claimant received bills from Cableuropa despite not having an account with them.	By virtue of Article 45.2 and 45.4 of LOPD, the SDPA imposed a fine of €50,000 on Cableuropa for breach of Article 6.1 of LOPD (not having consent from the data subject for the processing of personal data), classified as a serious breach by Article 44.3. b) of the LOPD
08 March 2013	Staples Productos de Oficina S.L.U	The claimant received a large quantity of unsolicited marketing emails despite not having authorised this and despite having twice requested that Staples stop sending these emails to the claimant.	By virtue of Article 40 of LSSI, the SDPA imposed a fine of €30,001 on Staples for breach of Article 21 of LSSI (sending commercial emails without consent) classified as a serious breach by Article 38.3. c) of the LSSI.
22 March 2013	Telefonica Moviles España S.A	In December 2010, Telefonica began to bill the claimant's current account for mobile phone services that she had not requested. Despite contacting Telefonica to ask for the service to be cancelled, the situation continued and the claimant was sent a bill from ISGL Informes Comerciales	By virtue of Article 45.5 of LOPD, the SDPA imposed a fine of €20,000 on Telefonica for breach of Article 6 LOPD (not having consent from the data subject for the processing of personal data), classified as a serious breach by Article 44.3. b).
03 April 2013	Vodafone España S.A	After settling a debt with Vodafone, the claimant's data remained in its capital solvency archives.	By virtue of Article 45.2 LOPD, the SDPA imposed a fine of €50,000 on Vodafone for breach of Article 4.3 of LOPD (data must be updated and correct), classified as a serious breach by Article 44.3.c) of the LOPD.

Sweden

Date	Infringing entity	Details of infringement	Sanction(s) imposed
15 January 2013	The Swedish Police in Örebro County (the "Police")	The Police used personal data from its entry system to verify whether a police officer had made false representations regarding hours reportedly worked.	None. The DIB found that the Police could use such personal data to investigate the matter. There must, however, be an actual suspicion of false accounting.
12 February 2013	The Swedish union Unionen (the "Union")	The Union operated a website where members could apply for membership. If a person entered their social security number (*Sw: personnummer*), their name and address would automatically be displayed on the website.	The DIB ruled that displaying such information was not permitted and that the Union must change its website. The DIB encouraged all website owners to change their websites to follow this ruling.
15 February 2013	The Municipality of Söderhamn (*Sw: Söderhamns Kommun*) (the Municipality")	The Municipality used digital ID badges to record children's attendance at private preschools within the municipality of Söderhamn.	The DIB investigated and found that it would always be an intrusion on a person's integrity to register their attendance at school. The Municipality was ordered to stop this practice.
03 April 2013	Socialdemokraterna (the Swedish Social Democratic Party) (the "Party")	The DIB investigated the Party's processing of member data. During this investigation, the DIB found that the Party disclosed personal data to a company that used the information to sell lottery tickets	The DIB required the Party to: • cease such disclosures; or • obtain member consent for the disclosure of their personal data for this purpose. The Party appealed the DIB's decision to the administrative court, which agreed with the DIB's decision.

United Kingdom

Date	Infringing entity	Details of infringement	Sanction(s) imposed
14 January 2013	Sony Computer Entertainment Europe Limited	In April 2011, the Sony Playstation Network was hacked, compromising the personal information of millions of customers, including their names, addresses, email addresses, dates of birth and account passwords. Registered payment details were also at risk, although there was no evidence that this was accessed during the system breach. The ICO found that the data controller had failed to ensure that proper technical measures had been taken against unauthorised data processing prior to the hacking and that this contravention was likely to cause substantial damage or distress.	Monetary Penalty of £250,000
16 January 2013	Prospect	Prospect invited tenders for an electronic membership system. One of the bidders asked for live data for testing purposes. Prospect emailed 19,000 membership records, containing sensitive personal data, to an incorrect email address. To compound the error, the bidder had no need for the data, as it was the incumbent provider so already had access to the data it needed through other means.	Prospect require to give undertakings to minimise and anonymise the data shared with third parties where possible and to adopt policies for secure data transfer.
25 January 2013	Mansfield District Council	Mansfield's Revenues and Benefits Service repeatedly sent correspondence to a housing association that was not intended for it. This correspondence included personal data. The ICO took into account the mitigating circumstance of human error.	The council was required to give undertakings to: • provide training, including e-learning modules; • repeat training at intervals of no less than 3 years; • provide training to all staff including agency staff; and • maintain training records.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
15 February 2013	The Nursery and Midwifery Council	The Council lost three DVDs relating to a nurse's misconduct hearing. The DVDs contained identifiable personal information about and evidence from two vulnerable children. The Council was couriering the DVDs to the hearing venue for the nurse's fitness to practice tribunal. When the packages were received at the hearing venue, the DVDs were not in their boxes, although the packaging showed no signs of tampering. Extensive searches were carried out, but the DVDs were never recovered. An ICO investigation found that the DVDs had not been encrypted.	Monetary penalty of £150,000.
18 March 2013	DM Design Bedrooms Ltd	The Glasgow based company made thousands of unsolicited marketing calls to the public. It consistently failed to check whether individuals had opted out of marketing calls by signing up to the Telephone Preference Service. The company also failed to respond to most of the complaints it received from members of the public.	Monetary penalty of £90,000.
04 April 2013	East Riding of Yorkshire Council	This action from the ICO follows two separate incidents in 2012, in which personal data were inappropriately disclosed in the course of responses to subject access requests: • In the first incident, a Council employee disclosed personal data about one family in a written response to a different family; and • In the second incident, a student social worker mistakenly told a parent the name of the person who had referred the parent to social services.	The East Riding Council of Yorkshire undertook to: • Ensure that all employees whose role involved routine processing of personal data have regular data protection training; • Have all responses to subject access requests checked by trained staff prior to being issued; • By June 30 2013, review its data protection policy; • Regularly monitor compliance with that policy; and • Implement additional security measures to ensure that personal data is protected against unauthorised or unlawful processing, loss, destruction or damage.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
08 April 2013	Ray Butler of Butler's Estate Agents	Since 2010, the ICO has undertaken a targeted campaign to get estate agents to register under the DPA, as many estate agents and letting agents were previously unaware of their duty to register. The ICO contacted Mr Butler three times to remind him that he needed to register with the ICO, but all three reminders were ignored. Mr Butler was prosecuted and convicted under s17 of the DPA for failing to register with the ICO.	Mr Butler was fined £300 and required to pay £405 towards the costs of prosecution. He was also told to pay a £30 victims' surcharge.
26 April 2013	The Burnett Practice	The ICO investigated a breach of the DPA after a free web-based email address used by the Burnett Practice was hacked and patients were asked to provide their bank details by the hacker. The email address was used by the doctor's surgery to send invitations to patients to attend smear tests and to confirm their smear test results. No sensitive information was accessed by the hackers but the email account contained the email addresses of around 175 patients of the surgery.	The Burnett Practice undertook to: • Adopt a secure mode of communication to provide patients with their test results; • Not send clinical data via email unless the security of the data can be ensured; • Put in place a security policy to cover the transfer of patient data securely and to train staff about that policy; • Ensure that all employees whose role involves routine processing of personal data have regular data protection training; • Regularly monitor compliance with data protection and IT security policies; and • Implement additional security measures to ensure that personal data is protected against unauthorised or unlawful processing, loss, destruction or damage.

European data protection news

Belgium

New guidance on data breaches in Belgium

Cédrine Morlière, Associate, Bird & Bird (Brussels)

The Belgian Data Protection Commission issued security guidance aimed at preventing data breaches. This guidance follows serious data breaches reported in the Belgian press in December 2012, which concerned a Belgian public transport company's customer data which appeared to be accessible to the public via the Internet.

In order to prevent such data breaches, the Data Protection Commission recommends putting adequate security measures in place, using an example from the ISO/IEC 27002 as a template; or from the general guidance on security measures published on the Commission's website. For example, access to data available on a private Intranet via the general Internet should be preventable using combined security measures such as firewalls, Proxy/Reverse Proxy servers, translation of IP adresses and adequate parameters for routers. In addition, access should be analysed in order to detect unwanted access attempts.

In case of data breach, an adequate alert and management procedure should be in place, enabling personnel to identify the technical experts or managers who should be informed of the breach immediately.

According to the guidance, if the data breach results in a "public incident" (i.e. public leakage of private data), the Data Protection Commission should be informed of the causes and consequences of the incident within 48 hours. In addition, a public information campaign should be rolled out within 24-48 hours of notifying the Data Protection Commission.

The Belgian Data Protection Commission also announced its intention to reinforce the present legal framework. There is already a legal obligation on data controllers to implement adequate security measures pursuant to the Belgian Data Protection Act. However, the Commission does not consider that this obligation is being implemented seriously enough. The Commision will now lobby the Belgian legislator to make its recommendations on security measures legally binding.

In the meantime, in cases of negligence relating to security measures, the Data Protection Commission will make use of all of the legal means currently available to it to hold data controllers responsible and may report any serious issues to the public prosecutor with possible criminal sanctions as a consequence.

The guidance on security breaches aims to enable the public prosecutor to assess the seriousnesss of the breaches reported to them.

The Data Protection Commission finally reminds data controllers of the fact that they can be held liable for any civil damages resulting from a violation of the Belgian Data Protection Act, unless they can prove that they were not responsible for the damage caused.

Companies wishing to reduce the risk of security breaches should check whether their security measures meet the standards recommended by the Belgian Data Protetion Commission in its new guidance.

(Recommendation 01/2003 dated 21 January 2013).

China

Rules for the protection of the personal information of telecommunications and Internet users – Draft for comment

Grace Chen, Partner, Bird & Bird (Beijing) and Marcus Vass, Partner, Bird & Bird (Hong Kong)

On 10 April 2013 the Ministry of Industry and Information Technology (MIIT) issued the draft Rules for Protection of the Personal Information of Telecommunications and Internet Users (the "Draft Rules") for public comment, which should be submitted by 15 May 2013.

The Draft Rules were formulated in accordance with the Decision on Strengthening Protection of Network Information (the "Decision") issued by the Standing Committee of the National People's Congress on December 2012, along with the PRC Telecommunications Regulations and the Internet Information Services Administrative Measures. The Draft Rules are intended to apply to activities involving the collection of personal data in the course of providing telecommunications and Internet information services.

Definition of Personal Information

A user's 'personal information' in the context of the Draft Rules refers to any information collected by telecommunications operators and Internet information service providers (collectively "Operators") in the course of providing services that can singularly or in combination with other information be used to identify the user. This includes:

- Identification information, such as the user's name, date of birth, ID number and address; and
- Login information collected during the user's use of the services, including the user's number, account number, time and location.

Standards for Collection and Use of Information

The Draft Rules oblige an Operator to adhere to the principles of lawfulness, appropriateness and necessity when collecting and using user data in the course of providing services. The Operator is obliged to:

- collect or use user personal information only with the user's consent;
- formulate and publish rules for the collection and use of user data;
- clearly inform the user of:
  - the purpose, means and scope of collecting and using the personal information;
  - the applicable retention period(s) for the information;
  - the channels that may be used by individuals to inquire about and amend their information; and
  - the consequences of refusing to provide the information; and
- set up a mechanism for handling user complaints, publish contact information for receipt of user complaints and respond to complaints within 15 days of receipt.

The Operator is not permitted to collect user personal information beyond the scope of what is needed to provide the services; use user data for purposes outside the scope of the services provided; or collect or use user data by means of fraud, misrepresentation or coercion or in any manner that violates the law, administrative regulations or an agreement between the parties.

The Operators and their personnel are subject to strict confidentiality obligations with respect to the user data collected and used in the course of providing services. This information may not be disclosed, tampered with or destroyed, nor can the information be sold or provided illegally to another person.

An Operator is not permitted to entrust service-oriented tasks requiring direct interaction with users and involving the collection and use of user data to any third party that cannot protect the user data concerned. The Operator is also expected to take responsibility for monitoring, supervising and managing the work of its service providers with respect to the protection of user data.

Security Assurance Measures

The Draft Rules stipulate that an Operator is responsible for the security of the user data that it collects and uses in the course of providing services. Specifically, the Operator is required to adopt measures to prevent user data from being disclosed, destroyed or lost, to adopt remedial measures for any disclosure, destruction or loss that occurs; immediately report any serious breaches to the relevant telecommunications administrative authority and cooperate in any investigations by the relevant authorities.

The Operators are also obliged to provide training to its personnel on the technical and security responsibilities that are relevant to protection of user data, to conduct periodic inspections, to keep records of its handling of user data and to eliminate any information security issues uncovered in the course of such audits in a timely manner.

Penalties for Non-Compliance

The Draft Rules call for rectification of any breach within a certain time frame and warnings and fines, which range from up to RMB10,000 (€1,250) for minor offences and between RMB10,000 and RMB 30,000 (€1,250 – €3,750) for more serious offences. If warranted, offenders may face criminal liability.

Although the potential fines are relatively low, any breach of the Draft Rules would very likely be a breach of the Decision, which provides for other penalties (including but not limited to confiscation of illegal profits, revocation of operation permits and shutdown of websites).

Conclusion and Recommendations

Although the Draft Rules in their present form appear to be directed at telecommunications operators and Internet information service providers, it is anticipated that the Draft Rules are intended to provide implementation guidance for the Decision, which makes reference not only to network service providers, but also other enterprises that collect and use personal information as part of their business activities. As such it is possible that the scope of application of the Draft Rules will be broadened to incorporate other companies that collect and use personal information in the course of business. Companies that need to collect and/or use personal data in their business activities in China should review the Draft Rules carefully and consider taking this opportunity to provide comments and suggest changes to MIIT.

Czech Republic

Right to information versus the protection of privacy?
Andrea Jarolímková, Associate, and Vojtech Chloupek, Senior European Counsel, Bird & Bird (Prague)

On 8 February 2013, the salaries of all employees of the High Public Prosecutor's Office in Prague (the "**Office**") were published on the Office's website, together with names of respective employees. It transpired that not only salaries of public prosecutors, but also salaries of clerks and other personnel were published. The Czech Office for Personal Data Protection (the "**DPA**") swiftly initiated administrative proceedings and, in April 2013, imposed a fine of CZK 100,000 (approximately €4,000) for breach of the data protection law because the salaries of clerks and other personnel were published in addition to that information relating to public prosecutors.

The Office claimed that the fine was disproportionate considering the sanctions imposed by DPA. The Office argued that it had acted in compliance with the decision of the Supreme Administrative Court from May 2011 (5 As 57/2010-79). In that case, the Supreme Administrative Court declared that an employee in public administration being paid by the state is "the recipient of public funds" in the sense of the Act No. 106/1999 Coll., on the Free Access to Information and therefore their personal data (name, surname or remuneration) can be published. As far as the conflict between the right to information and the protection of privacy is concerned, the court merely said that the right to protection of personal data was not unlimited.

The DPA strongly criticises the Supreme Administrative Court for failing to apply the proportionality test and ignoring data protection law. As a result of the unsatisfactory reasoning, it inevitably follows from the decision that the salary of each employee in public administration can be published in any circumstances and without exception. This is perceived by the DPA as discriminatory against employees paid from public funds, such as teachers, doctors, nurses, policemen etc. The salaries of these individuals were published without considering their right to protection against such processing by means of a constitutional complaint.

In the past, the DPA warned that the present judgment might serve as an incentive for blanket disclosure of salaries of all public administration employees irrespective of the interest in protecting their private life, as happened in the case of the Office. In line with the Constitutional Court's decision and the case law of the European Court of Human Rights, the DPA expressed its intention to apply the proportionality test on cases of the blanket publication of public administration employees' salaries. If public interest does not prevail over the particular employee's right to protection of their privacy, the DPA would apply sanctions.

Interestingly, the DPA is not alone in having problems accepting the results of the controversial judgment of the Supreme Administrative Court. In August 2011, a meeting of representatives from the Ministry of the Interior, the DPA, the Ministry of Justice, the Office of the Ombudsman and the Open Society, and a non-profit organisation took place to formulate a non-binding recommendation of the Ministry of the Interior on providing information about salaries of employees. Most importantly, the recommendation stipulated that in principle the judgment does not exclude the applicability of the proportionality test in reasoned cases. It suggests certain criteria to be taken into consideration, for instance, whether the employee has decision-making power or whether have larger public funds at their disposal. The recommendation also stipulates that the information should be made anonymous if published on the internet, unless it concerns the highest management of the public administration.

As the Office is to use a remedial measure against the DPA's decision by which the fine was imposed, it is going to be highly interesting to observe how the present case concerning the conflict between the right to information and the right to the protection of privacy will continue.

France

French Data Protection Authority unveils its 2013 targets for inspections
Ariane Mole, Partner, Bird & Bird (Paris)

In 2012, the French Data Protection Authority ("**CNIL**") carried out 458 on-site inspections as part of its programme focussing on mobile phone operators, processors of health data and customer databases and the police. This was a 19% increase on the number of inspections carried from 2011 and it came in addition to other controls following complaints received. The CNIL received 6,000 complaints in 2012. 137 of the CNIL's on-site inspections concerned CCTV systems.

The CNIL's annual programme for 2013 was adopted on 28 February 2013 and published on 19 March 2013. The CNIL set an objective of achieving around 400 inspections this year. A quarter of the CNIL's inspections will relate to CCTV systems. According to the CNIL, a third of inspections will be reserved for the investigation of complaints received.

The CNIL will focus on the following issues in its programme of inspections for 2013:

- **25% of the inspections will relate to CCTV systems:** As in 2012, the CNIL will focus on CCTV compliance as French law was recently amended to provide more powers to the CNIL for such systems.
- **Data processing by market research companies:** The CNIL's action in this area will provide it with a clear idea of how the data is used and will allow the authority to advise market research companies on any corrective actions that they need to take.
- **Data processed by hotspots offering free Internet access (e.g. Wi-Fi hotspots):** A large amount of very precise data is produced by the use of these services by a growing number of people (e.g. internet browsing history, private correspondence and traffic data retained for law enforcement purposes). The checks to be carried out by the CNIL will aim to ensure that the legal framework for the retention of such data is respected.
- **Processing by local authorities of data relating to persons' social difficulties:** The CNIL will carry out inspections of *communes*, CCAS boards and councils, focussing on the strong challenges which such bodies face in terms of the protection of the data that they process about people in difficult social situations. Such challenges include data security, the sharing of information between different entities and data retention. The CNIL aims to ensure that controllers fully respect the rights provided by law in relation to such data.
- **Data about persons detained in prison:** The CNIL's checks in this area will allow it to assess the conditions under which data kept by prison authorities is used. Such data includes the national file of prisoners, CCTV and possible electronic surveillance during provisional release.
- **Police files:** The CNIL will also monitor the operational services of the police and gendarmerie in order to see first-hand how police files are used. This idea was already included in the CNIL's programme in 2012.
- **International enforcement actions:** Another main theme for the CNIL in 2013 will be international cooperation on investigations between data protection authorities. According to the CNIL, if there is already some international cooperation in a certain area (such as the ability to ask another European DPA to carry out an investigation, or carrying out an investigation which another European authority asked it to) the CNIL is keen to increase its activity in this area, in line with the recommendations in the proposed new EU General Data Protection Regulation.

France releases data protection recommendations for Smart Meters under the direct control of customers

Gabriel Voisin and Joshua Partridge, Associates, Bird & Bird (UK)

In January 2013, the CNIL issued initial recommendations to regulate the use and deployment of smart meters following a two year review on this issue. Smart meters will start being deployed across France in 2013 and, by 2020, should be installed in approximately 35 million homes.

The CNIL reports that smart meters pose potential issues in terms of security and privacy, with the 'load curve' singled out for specific attention. The load curve takes regular measurements of usage, allowing for detailed and accurate information on the lifestyles of the residents of a particular home to be gathered. This data could be used to determine, amongst other things, time of peak usage and, of more concern, wake-up and bed times or times when the home is regularly empty.

In light of these issues, the CNIL has proposed initial recommendations for the regulation of smart meter use, which were adopted on 15 November 2012 following consultation with the *Commission de régulation de l'énergie* (CRE) and *Conseil Général de l'Economie, de l'Industrie, de l'Energie et des Technologies* (CGEIET).

The recommendations set out that the load curve may only be measured systematically where justified as necessary to maintain the electricity network or where explicitly requested by the consumer in order to benefit from services such as price adjusted consumption, which relies on detailed and regular data collection. The recommendations also set out security requirements for consideration and call for privacy impact assessments to determine the appropriate measures needed.

The CNIL also aims to address issues raised by smart technologies not being placed under the direct control of customers (e.g. in the operator's electric meter located at a street level). To assist it in this role, the CNIL has formed a partnership and working group with *the Fédération des Industries Électriques, Électroniques et de Communication* (FIEEC) in order to set out best practices in the industry, which are due to be released in the summer of 2013.

More information can be found (in French) at the following address: http://www.cnil.fr/la-cnil/actualite/article/article/compteurs-communicants-premieres-recommandations-de-la-cnil/

A new tax on personal data collection?

Gabriel Voisin, Associate, Bird & Bird (UK)

In July 2012, the French government commissioned Pierre Collin and Nicolas Colin (the Rapporteurs) to identify measures addressing what is seen as tax avoidance by digital companies. On 18 January 2013, the Rapporteurs issued their Report, which can be found (in French) here. The report suggests acting on two different levels.

International Scale

The report firstly suggests redefining the notion of a "permanent establishment" provided for by the Organisation for Economic Cooperation and Development (OECD), to which the taxation of all companies within the Member States are subject. The report proposes to take into consideration the so-called "free work" of users which, in providing their data, form a strategic source of revenue for digital businesses. The OECD has already been involved in such work on multinational taxation. This stream of revenue could come to an end between 2013 and 2014.

French Scale

In the meantime, the Rapporteurs suggest legislating at a national level, proposing taxation based on the collection and use of personal data in France.

1. Rationale

The report suggests that some digital companies pay very little tax in countries where their users are based. Therefore, according to the Rapporteurs, the added value created should be taken into account when they state their profits in a country. According to the Report, tax

authorities should at least take care to limit the transfer of profits between subsidiaries of a group in different countries.

From the Rapporteur's point of view, the ability to gather users and collect data is an asset, which is locally taxable as it can be linked to a permanent establishment. However, this new tax might be difficult to implement as not all data is uniform: the value varies greatly according to source, rarity, use, etc. In this respect, the Rapporteurs recognise that no economist interviewed while preparing the Report has been able to propose a method to isolate the share of value coming from processing of personal data of users, for any given business.

2. Creation of a model

However, according to the Rapporteurs, tax authorities should tackle this new challenge. For the Rapporteurs, market data on the digital economy already exists (e.g. data coming from intelligence services, financial communications services). Additionally, tax authorities could rely on academic research to create a new comparative model for the valuation of data.

The Rapporteurs suggest this new tax should be experimented upon the biggest contributors. The proposed tax would be used "only above a certain threshold in the number of users, to be determined", so as not to penalise start-up businesses. Under guidance from the tax administration, the business will itself quantify the volume of data that it collects and uses. According to the Report, taxation would be made in the form of a single tariff per user, which could vary according to the behaviour of the business (e.g. compliance towards data protection, data security and data portability). The approach is being presented by the Rapporteurs as "an incentive" and should not be viewed as a means of financial gain.

Next steps

A follow-up to the Report is yet to be decided. Two legislative initiatives might offer a window for the proposal to go further:

- Draft legislation on a neutral and fair digital tax (first public discussion to be held before the French Parliament on January 31, 2013. More information can be found here); and
- The Annual Budget Proposal to be discussed before the French Parliament in Autumn 2013.

Hungary

Hungary removes sub-processing prohibition

Bálint Halász, Associate, Bird & Bird (Budapest)

The Hungarian Parliament passed an amendment removing the prohibition of sub-processing from the Hungarian Privacy Act. The amendment will enter into force on 1 July 2013, resulting in a clear platform where outsourcing will not trigger any unnecessary legal risks. The amendment is a significant step towards updating Hungarian data protection legislation, implementing both European legislation and recent technology trends.

The previous preclusion of sub-processing

Both the previous Hungarian law and the current Data Protection Act (Act 112 of 2011), which entered into force on 1 January 2012, contained an outdated provision which expressly precluded sub-processing (i.e. the outsourcing of processing functions by a processor to a sub-processor). This requirement clearly conflicted with the needs of the cloud computing industry, not to mention EU law (for example, Commission Decision 2010/87/EU on Standard Contractual Clauses for the transfer of personal data to processors established in third countries, which enables sub-contracting provided certain criteria are met). The former Data Protection Commissioner had stated that EU law should prevail in the case of a conflict between Hungarian and EU law. However, this interpretation has not been confirmed by the courts, and the Data Protection Act as it stands retains the exclusion. The head of Hungarian Data Protection Agency (NAIH) issued an opinion in which he admitted that the provision conflicted with European law and sub-contracting should be allowed. Nevertheless, until the Data Protection Act is not amended, statutory law cannot be disregarded.

The new provision entering into force on 1 July 2013

While it is expected that the Hungarian Data Protection Act will be revised in the course of 2013 in order to make it compliant with European legislation and case law, the amendment above is not part of this long-awaited comprehensive amendment but instead is a new act addressing data security in the public sector. The Act on the Electronic Information Security of Public and Municipal Bodies (Act 50 of 2013) was passed by the Hungarian Parliament on 15 April 2013 and published in the Official Gazette on 25 April 2013. Article 28 of this act amends Article 10(2) Hungarian Data Protection Act by stating that a processor is allowed to engage a sub-processor in accordance with instructions of the controller.

Comments

For several years stakeholders have been urging both the previous data protection commissioners and the Hungarian Data Protection Agency to lift the outdated preclusion of sub-processing as it was considered an unnecessary burden for businesses processing personal data: it clearly conflicted with cloud computing and other recent technological developments.

In January 2013 Mr. Attila Péterfalvi, president of the NAIH, announced that the Hungarian Privacy Act would be significantly amended in 2013 and one of the amendments would affect the prohibition of sub-processing. By amending and replacing this provision, the Hungarian legislator acknowledged that the preclusion of sub-processing was outdated and it is essential to update the Hungarian Data Protection Act in order to restore Hungary's competitiveness in cloud computing and to keep up with recent technological trends, European legislation and case law.

Italy

Authorisation from the Garante to the use of biometric data in the context of a digital signature system

Debora Stella, Associate, and Valentina Gallinelli, Trainee, Bird & Bird (Milan)

In light of the intention to promote a *"growth in the quality of its services' delivery"*, two major Italian banking institutions declared they wanted to benefit their customers by making available a document subscription service with a digital signature. The service would be based on a biometric authentication procedure performed by SignPad, intended to confer greater safety in the performance of traditionally counter-type transactions, ensuring *"greater security against attempted fraud"* by reducing *"the risk of identity theft and signature counterfeiting"*. The system would collect the customer's biometric behavioural characteristics by detecting and analysing some parameters related to the customer's signature (rhythm, speed, pressure, acceleration and motion) in order to compare these characteristics against those collected from the customer when signing up to the service. Any positive comparison, which would lead to user authentication, would enable the digital signature of the document to be seen by the customer.

The Garante considers the processing of this biometric data acceptable, according to the documents submitted and to the statements made. In fact, the positive and rigorous identification of the customer is an obligation for all credit institutions, usually imposed through sector-specific regulations (and informally required by banks as a means of prudent risk management). The violation of these regulations can be a source of civil liability, as per Article 1176 of the Italian Civil Code.

Where the processing of biometric data of the signatories, to the extent that it may be considered to be compatible with the current regulatory framework applicable to digital signature services, will be based on the free consent of the parties and the pursuit of legitimate purposes made known in advance to the customer, the requirements laid down in Articles 11, 13 and 23 of the Italian DP Code are complied with.

The biometric authentication of customer digital signatures could help to effectively counteract attempted fraud and streamline and speed up the operations of customer recognition at the counter.

Data breach notification obligation for telephone companies and internet service providers

Following a public consultation, the Garante adopted a provision which implements the European Directive on privacy in the electronic communications, establishing the arrangements for data breaches.

Telecoms companies and internet service providers are obliged to notify the Garante and their users when the data processed to provide the services is subject to serious violation as a result of cyber-attacks or adverse events, such as fires or other disasters, which could lead to the loss, destruction or undue dissemination of that data.

Telecoms companies and ISPs, as well as companies providing e-mail services and mobile payment services, must notify the Garante with the necessary information to enable an initial assessment within 24 hours of the discovery of the event. The extent of the violation must be outlined in that report. To facilitate breach reporting, the Garante has drafted a template report form, available on its website.

In cases of serious violations, telecom companies and ISPs will also have to inform each user concerned within three days of the violation. Communication to the users is not required if the telecoms company or ISP has proved to have used security measures and data encryption/an anonymisation system to render the data unintelligible.

Moreover, telecom companies and ISPs will have to keep a constantly updated inventory of the security violations that it has been involved in.

Failure or delay in informing the Garante will lead to an administrative penalty ranging from €25,000 to €150,000. Penalties for failure to notify users range from €150 to €1,000 for each company, entity or person concerned. Failure to maintain an updated inventory may be subject to a fine of €20,000 to €120,000.

Poland

Are e-service providers allowed to disclose IP addresses of their users to private parties?

Izabela Kowalczuk, Associate, and Krzysztof Korwin-Kossakowski. Trainee, Bird & Bird (Warsaw)

Until very recently, the Voivodship Administrative Court in Warsaw ("Court") has not challenged the right of e-service providers to disclose user IP address to private parties based on the Polish Personal Data Protection Act (PDPA). This has changed, however, as the Court issued two judgments stating that e-service providers (website operators) are not allowed to disclose such data (judgment dated 31 January 2013, case no. II SA/Wa 1112/12 and judgment dated 8 March 2012, case no. II SA/Wa 2821/11). Neither judgment is yet conclusive.

Background

In both cases, a user posted content infringing the goodwill and personal rights of other private parties on the e-service providers' website. The affected private parties requested the e-service providers to disclose the IP address of the publishers in order to sue them. The e-service providers refused, so the private parties filed complaints with the GIODO.

GIODO's decision

GIODO ordered the e-service providers to disclose the requested personal data:

- In case no. II SA/Wa 1112/12, GIODO decided that disclosing the IP address was in the legitimate interests of data recipients and that such processing did not violate rights and freedoms of users (Art. 23 sec. 1 point 5 of the PDPA); and
- in case no. II SA/Wa 2821/11, GIODO based its decision on the already-repealed Article 29 of the PDPA.

The e-service providers filed complaints with the Court.

Ruling

The Court agreed with the e-service providers and explained that the Act on Providing Services by Electronic Means (E-Service Act) distinguishes (i) users' personal data and (ii) users' operational data (which includes IP addresses). The E-Service Act regulates operational data separately and refers to the PDPA only in relation to personal data. Article 18 sec. 6 of the E-Service Act stipulates that e-service providers are obliged to disclose both categories of data only to state authorities for the purposes of court proceedings.

Since the PDPA does not apply to operational data, on the basis of Article 18 sec. 6 of the E-service Act, e-service providers can only disclose IP addresses of their users to the state authorities and not to private parties based on the legitimate interest condition (Art. 23 sec. 1 point 5 of the PDPA) or Article 29 of the PDPA.

The Court also indicated that the private parties could have used other legal means to establish the requested data. For example, they could have obtained personal data through proceedings on securing evidence under the Polish Civil Procedure Code.

GIODO's position

Art. 18 of the E-Service Act should not be understood as prohibiting the disclosure of any personal data (including IP addresses) to any private party. If the legislator wished to introduce such prohibition, the relevant law would explicitly state that the data can be disclosed to state authorities "exclusively". Therefore, the e-service provider may disclose the IP address to private parties under the PDPA.

Comment

E-service providers can benefit from these judgments and rely on them to avoid disclosing user IP addresses without even analysing whether a request is justified. However, the Court's line of interpretation hinders the enforcement rights of individuals/entities whose rights were infringed online. They need to seek other limited alternatives (e.g. criminal proceedings). In comparison to an offline environment, this interpretation leads to the discrimination of individuals/entities that request data disclosure in relation to online infringements.

It should be highlighted that the situation is unclear as there are conflicting judgments from the same Court from late 2012 stating that the provisions of the PDPA can be a valid legal basis for e-service providers to disclose personal data to private parties (for example the judgment of 15 November 2012, case no. II SA/WA 1511/12). GIODO supports this line of interpretation.

Slovakia

Update on the new Slovak data protection legislation

Radovan Repa, Bird & Bird (Bratislava)

Pursuant to the press release dated 5 April 2013, published on the website of the President of the Slovak Republic, the President did not sign the new Slovak data protection Act ("the new Act") but returned it to the Slovak Parliament for a further discussion, proposing several new amendments to the new Act for approval by the Slovak Parliament.

The President does not agree with the transitional provisions regarding the cancellation of the existing:

- authorisation and notification of the appointment of data protection officers ("DPO") made by controllers and granting a year-long transition period to controllers to appoint and notify newly appointed DPOs to the DPA pursuant to the new Act and rather strict requirements comprising (e.g.) an examination of their knowledge from data protection legislation by the DPA; and
- registration of the filling systems made with the DPA; instead granting a 6 month transition period for new registrations of all filling systems pursuant to the newly introduced registration procedure.

The President proposes to deem the currently appointed and notified DPOs as DPOs meeting the criteria set in the new Act, in order to prevent a situation where DPOs are appointed in compliance with data protection laws during the transitional period. The President's proposal also enables these DPOs to avoid the new requirement of examination of their knowledge of data protection laws by the DPA.

In case of the registration of filing systems, the incorporation of the President's proposal would result into savings on costs incurred by controllers that have already registered their filling systems and related to the newly proposed administrative fees in the amount of €20 for a registration and €50 for a special registration of the filing system (i.e. filing systems containing special categories of personal data).

The President proposes to postpone the effectiveness of the new Act from 1 June to 1 July 2013. Other amendments are predominantly of a technical nature and do not significantly alter the wording of the new Act that was already approved by Parliament.

Spain

Spanish Data Protection Agency issues Guides on Cookies and Cloud computing

Javier Fernández-Samaniego, Partner, Bird & Bird (Madrid)

Following the Spanish Data Protection Agency's ("SDPA") 5th Open Doors Annual Meeting, a Guide on the Use of Cookies and two Guides on Cloud Computing for Users and for Service Providers have been issued by the Spanish DP Supervisory Authority.

Guide on the Use of Cookies

This is the first European guideline drafted between industry and the Supervisory Authority. It was jointly drafted with industry associations Adigital (e-commerce association), Autocontrol (self-control advertising association) and IAB Spain.

Since the Spanish implementation of Directive 2009/136/EC in March 2012, the lack of guidance on how the new Article 22.2 of Law 34/2002 ("Spanish E-Commerce Act") should be applied by websites had led to a general non-application of this law. With the issuance of this Guide, the SDPA tackles the main controversial issues surrounding how the cookies regulation must be applied: the ways in which the statutory information on the use of cookies must be provided, the ways of obtaining a user's consent, and how this applies to third party cookies.

Information on the Use of Cookies

Regarding the statutory information on cookies that must be offered according to the Spanish E-Commerce Act, the SDPA has established that this information may be given in a number of different ways:

- Offering the information in the header or footer of the website;
- For registered users, through the Terms & Conditions of the website;
- Through a banner that offers some basic information (a "first layer"), that must include: the use of non-exempt cookies, the specification of their purposes and of the existence third party cookies, information on the action by which consent to the use of cookies may be implied, and a link to the cookies policy ("second layer").

The cookies policy shall include: the definition and function of each cookie; information on the types of cookies used; information on how to delete the cookies; and identification of the party that places the cookies (the editor or third parties).

Consent

Through this Guide, the SDPA has formally accepted users' implicit consent for the use of cookies. However, this implied consent must be given through some kind of specific action: the SDPA expressly excludes that the user's inactivity implies consent for the use of cookies.

Specific examples on the ways by which implicit consent may be valid are offered by the SDPA: the use of the scroll bar if the cookies information was visible before moving it; or if the user has clicked on any content of the website.

Other ways of obtaining consent mentioned by the SDPA are:

- accepting the website's T&Cs or privacy/cookies policy;
- through the configuration of the website's functionality (Settings-led consent);
- the moment at which a new function is offered on the website (Feature-led consent);
- before downloading any specific content offered in the website; and
- through the configuration of the browser.

Third Party Cookies

Regarding the debate about who must provide the statutory information and collect the user's consent when the cookie is placed by a third party, the SDPA considers that both the owner/editor of the website and the third party are responsible for providing the statutory information and for obtaining consent. The SDPA also suggests that complying with this may be easier for the owner/editor of the website, and considers that these issues should be covered in the contract between both parties.

Cloud Computing Guides

The SDPA has also issued a "Guide for Clients that Contract Cloud Computing Services", and a "Guide for Cloud Computing Providers".

In the Guide for Clients, the main issues that arise regarding Cloud Computing Services are explained to users from a Data Protection point of view: the possibility that the services are provided from places that are not considered adequate from a Data Protection perspective, the specifications that must be in the contract in order that the cloud provider may subcontract the services, issues regarding accountability and portability of the Data, and the main risks that may come up from the use of Cloud Computing. The final section of the guide is intended to provide certain guidelines to Public Administrations on the contracting of Cloud Computing.

In the Guide for Cloud Providers, the main Data Protection legal issues are also summarized to offer some basic guidelines to Cloud Providers regarding the Data Protection legislation, as they will act as data processors of the client's data. In addition, although it is not explained in this Guide, on November 2012 the SDPA published Standard Contractual Clauses for transferring data from processors located in Spain to subprocessors located in third countries, a mechanism that may be very useful for Cloud Providers.

UAE

UAE Cyber Crime Law 2012

Melissa Murray, Bird & Bird (Abu Dhabi)

Towards the end of 2012, an updated Cyber Crime law was issued at a UAE Federal level, repealing the previous 2006 Cyber Crime law. The new law covers a range of crimes found in the use of electronic and information technology tools.

Various articles of the updated Cyber Crime Law provide specific data protection offences, including imprisonment and fines for things such as:

- capturing information (including documents, signatures, etc.) using fraudulent methods through an information network or system;
- unlawfully obtaining banking information (with higher penalties for actual use of the information);
- intercepting, transferring, recording, transmitting or disclosure of conversations, communications or audio/visual materials.

At this stage, the UAE does not have a specific data protection law, but the updated Cyber Crime Law provides further data protection offences in addition to provisions in others UAE laws which relate generally to data protection and privacy of information.

DIFC Updated Data Protection Law

The DIFC (Dubai International Financial Centre) is a financial free zone located within Dubai, UAE. The DIFC is one of the few jurisdictions in the Middle East with its own data protection laws. At the end of 2012, the DIFC amended its Data Protection law through the Data Protection Amendment Law No 5 of 2012. The amendments are mainly administrative, however there is now a formal system of fines for various contraventions which was previously missing.