# International data protection enforcement bulletin – April 2014

Welcome to the April 2014 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, highlights up to January 2014 include:

- An investigation in Hong Kong on the leaking of internal documents by the Hong Kong Police Force, and a summary of the Hong Kong Data Protection Authority's work in 2013 as well as plans for 2014
- The Czech Data Protection Authority clarifies its position on phone call records
- The Polish government's discussions on reducing requirements for data transfers to third countries

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


Ruth Boardman
Partner
ruth.boardman@twobirds.com

Ariane Mole
Partner
Ariane.mole@twobirds.com

# Enforcement tables by country

## China

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **30 November 2013** | **Mr. Zhou** (an individual) | Mr. Zhou was charged and held criminally liable for illegally obtaining personal information of citizens due to his purchasing citizens' personal information such as residency and cell-phone communication materials, through the internet from criminals and making a profit of more than 50,000 RMB via his private detective agency. | Guangdong Province Guangzhou City Tian He District People's Court issued a judgment in the first instance sentencing Mr. Zhou to one year's imprisonment and imposing a fine of 20,000 RMB (approx. **EUR 2,400**). |
| **30 November 2013** | **Mr. Miao Shirui** (an individual) | Mr. Shirui was held criminally liable for purchasing large volumes of citizens' personal information for use in his surveillance and investigation business operations. | Guangdong Province Guangzhou City Tian He District People's Court sentenced Mr. Shirui to 10 months in prison and imposed a fine of approx. **EUR 1,200**. |
| **December 2013*** | **Mr. Wei** (an individual) | Mr. Wei illegally obtained citizens' personal information from the internet and resold the personal information multiple times, making profits totalling more than 300,000 RMB. | Gansu Province Bai Yin City Ping Chuan District People's Court issued a judgment in the first instance sentencing Mr. Wei to **one year and six months' imprisonment suspended for two years**. |
| **December 2013*** | **Mr. Li** (a policeman) | Mr. Li was a policeman with the public security bureau in Foshan who took advantage of his job position to conduct searches in the PSB's internal network for citizens' personal information, information about fugitives, and information about detained individuals persons, taking photos of the aforementioned information and transmitting them through cell phone communication to a Mr. Wang of Hong Kong who was temporarily residing in Foshan. Mr. Li was found to have illegally provided to Mr. Wang more than ten items of citizens' personal information. | Guangdong Province Foshan City Chan Cheng District People's Court issued a judgement sentencing Mr. Li one year's imprisonment and imposed a fine of 20,000 RMB (approx. **EUR 2,400**). |

*We were unable to find information concerning the exact date on which the decision was handed down by the court.

# Czech Republic

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **October 2013** | **SOLUS** | Association SOLUS, a non-banking organisation, operates a debtor register. SOLUS failed to erase the data of two debtors listed in the register who withdrew their consent to personal data processing. As the Czech law does not regulate operation of debtors' registers by such kind of organisation, there is no particular legal title for processing of personal data. Therefore, the general DP rules apply. | The Authority imposed a fine of CZK 20,000 (approx. **EUR 730**) and in the second instance upheld that:<br>• personal data of debtors can be listed in the register only with the consent of a debtor,<br>• each debtor has right to withdraw the consent with the processing of his personal data and then SOLUS is obliged to remove his data from the debtor register. |
| **December 2013** | **KB Penzijní společnost, a.s.** | In the period between 21 May and 23 July 2013, pension management company KB Penzijní společnost made accessible via the "MyBank" internet portal, the internal database with the personal data of at least 45, 645 people interested in pension products to its clients. | The Authority imposed a fine of CZK 1,800,000 (approx. **EUR 65,360**). |

# France

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **25 September 2013** | CNIL's injunction to **Hospital of the city of Saint Malo** | The CNIL carried out an on-site inspection of the hospital of the city of Saint Malo following articles in the press concerning the processing of health data information systems by external processors.<br><br>The on-site inspection revealed that medical data covered by medical secrecy were processed by processors which were not part of the hospital staff but third parties.<br><br>The hospital explained why, because of the cost of medical data processing, they had to call upon external processors in order to process data more efficiently and for a lower cost.<br><br>Nevertheless, the CNIL considered that because the external processor were neither part of the hospital's staff, nor subject to medical secrecy, its access to the data was illegal and that, in order to be legal, it should have been systematically monitored by a doctor in the hospital, or by someone else who was part of the hospital and also subject to medical secrecy.<br><br>The CNIL thus considered that the hospital failed to comply with its obligation of data security and to respect individual's privacy (respectively under article 36 and article 1 of the French Data Protection Act), and the CNIL issued an enforcement notice to the hospital to stop using the external processor.<br><br>This decision is likely to raise issues for hospitals since working with external processors is common practice and hospitals cannot always afford to process data internally. | The CNIL decided to make public the **formal notice** to Saint Malo's hospital requiring the hospital to stop allowing the outsourced processing of health data by external processors, within a period of 10 days.<br><br>The hospital complied and the CNIL did not sanction the hospital. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **24 October 2013**<br>***(2 decisions)*** | CNIL's sanction to **Nouvelle Communication Téléphonique (NCT) and the AOCT company** | In April 2011, the CNIL received a complaint regarding the CCTV system in stores operated by 2 companies NCT and AOCT, run by the same manager.<br>Since the two companies did not answer the CNIL's letter, in October 2012, the CNIL decided to carry out on-site investigations of the two companies. The site manager being opposed to the control refused to let the CNIL enter the premises, therefore the CNIL came back in November 2012 with a specific court authorization to perform its investigation with the police assistance.<br>Following the on-site investigation, the CNIL ordered NCT and AOCT to comply with their obligations under the French Data Protection Act.<br>The CNIL considered that NCT and AOCT failed with their obligations of:<br>• notifying the CCTV processing to the CNIL (article 22 of the French Data Protection Act);<br>• informing the data subjects (article 32 of the French DP Act);<br>• providing data security; and<br>• responding to the CNIL questions and enforcement notice. | NCT was fined **EUR 10, 000** and the decision was **made public**.<br>AOCT was also fined **EUR 10,000** and the decision was **made public**. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **23 November 2013** | CNIL's sanction to **Abers Production Incendie** | In September 2011, the CNIL received a complaint from an employee of Abers Production Incendie regarding the conditions of the implementation of a geolocation device on employees' vehicles.<br><br>The employee complained that:<br><br>• the geolocation device was also used in order to control employees' schedules and that this purpose has neither been declared nor brought to the employees' attention; and<br><br>• there was no possibility to disable the geolocation device after working hours.<br><br>Despite several letters, on January 2012 the CNIL received two others complaints about the same device.<br><br>The CNIL asked Abers Production Incendie details about the implementation of the geolocation device and its purposes and, on November 2012, the CNIL ordered Abers Production Incendie to comply with the obligations of the French Data Protection Act. | The CNIL considered that Abers Production Incendie failed with requirements to:<br><br>• comply with the commitments of its notification declared to the CNIL since the device as implemented was used for monitoring employees' activities, contrary to what was declared in its notification with the CNIL; and<br><br>• respond to the CNIL's enforcement notice.<br><br>Abers Production Incendie was fined **EUR 3,000** and the decision was **made public**.<br><br>(Note: the fine was not EUR 10,000 as requested by the rapporteur, as some of the CNIL's requirements had been complied with following the CNIL's enforcement notice). |
| **12 December 2013** | CNIL's sanction to **ASC Groupe** | In June 2012, the CNIL received a complaint from several employees of ASC Groupe regarding the implementation of a CCTV system in the company's offices without any employee information notice.<br><br>The company answered that employees had been noticed and that the processing was implemented in order to prevent theft and intrusion.<br><br>The CNIL then asked the company to register the processing and to produce a copy of the information notice to employees.<br><br>The CNIL reminded ASC Groupe of their obligations under French Data Protection law on several occasions and did not receive a response. Therefore, in April 2013, the CNIL issued an enforcement notice which was also left without response from ASC. | The CNIL considered that ASC Groupe failed with its obligations to:<br><br>• notify its processing with the CNIL (article 22 of the French Data Protection Act);<br><br>• inform of the data subjects (article 32 of the French DP Act); and<br><br>• respond to the CNIL's requests and enforcement notice.<br><br>ASC Groupe was fined **EUR 10,000** by the CNIL and the decision was **made public**. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **14 January 2014** | Ruling from the French Supreme Court:<br><br>**Transports Goubet / M.X** | A truck driver was fired because he had tampered with the electronic tachograph placed in his professional truck in order to record speeds and driving times.<br><br>The first court and also the Court of Appeal had considered that since the implementation of the tachograph was not notified to the CNIL, the data processed with such device were unenforceable against the employee. Therefore they ruled that the dismissal had an illegitimate cause.<br><br>These decisions were consistent with existing French case law, according to which failure to register with the CNIL on the processing of employees' data results in non-enforceability of the processing of such data against employees. This also applies in case of failure to inform employees of the processing of their data.<br><br>The employer appealed of the Court of Appeal's decision to the Cour de Cassation (the French Supreme Court).<br><br>The French Supreme Court overruled the Court of Appeal's decision, considering that, in this specific case, despite the lack of notification to the CNIL, the employer was entitled to use the data collected by means of the tachograph against his employee, on the ground that implementation of a tachograph was a legal obligation under European Regulation (n°3821/85 and n°561/2006). According to such Regulation, employers are required to install a tachograph in the trucks and a failure to comply with such requirements is a criminal offence. Therefore the Supreme Court made an exception to its existing case law on the ground that because the tachograph is a legal requirements, its existence should be known by the employees despite the absence of notification to the CNIL and despite information notice to employees. Thus it is enforceable against employees.<br><br>By this new decision, the French Supreme Court operates a distinction between processing of personal data resulting from a decision of the employer and processing of personal data required by law. In the first case, the notification of the processing to the CNIL is an essential condition for the legal existence of the processing and thus of its enforceability against employees. In the latter case, the legal existence of the processing and its enforceability towards employees does not depend on its notification to the CNIL.<br><br>This decision does not, in any way, affect the obligation to notify the processing of personal data to the CNIL. Even though the tachograph is legally mandatory, it still results in processing of the driver's personal data which, as such, must comply with French DP law. Therefore, the employer could be sanctioned by court or by the CNIL for lack of notification to the CNIL or to the employees. But failure to notify does not trigger a non-enforceability of the device against employees, in the specific context where the device is mandatory by law. | |

# Germany

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **April 2013** | **Google** | The DPA of Hamburg sanctioned Google for unlawful recording of data from Wi-Fi networks when rolling out its Google Street View service. | The DPA of Hamburg imposed a fine of **EUR 145,000** upon Google. |
| **June 2013** | **Employee (name of company was not made public)** | An employee of a company has sent an email to a large group of recipients of an open mail list (instead of sending bccs). The Bavarian DPA took the opinion that email addresses (in particular those containing the first and surname of the recipient) qualify as personal data. The use of an open mail list was considered to be an unjustified transfer of personal data to third parties. | The Bavarian DPA imposed a fine upon the employee who sent the email (the amount was not made public). |
| **June/July 2013** | **Management (name of company was not made public)** | In a similar case, the same DPA also sanctioned the management of a company because it did neither instruct the employees to use bcc instead of open mail lists when contacting a group of different customers nor did the management supervise the employees accordingly. | The Bavarian DPA imposed a fine upon the competent managers (amount was not made public). |

# Hong Kong

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **31 July 2013** | **Glorious Destiny Investments Limited**<br><br>("**GDI**") | **Key facts:**<br><br>GDI collected litigation and bankruptcy data from the public domain and developed a database for a mobile app named "Do No Evil" (the "**App**"). The App allows a subscriber to view in one go a target individual's litigation, bankruptcy and directorship records, which include names, addresses, partial Hong Kong Identity Card numbers, action numbers and reasons for claims. The developer of the App claimed that it held a database of over 2 million litigation records.<br><br>**The findings of the Privacy Commissioner of Personal Data (the "Commissioner"):**<br><br>The Commissioner concluded that GDI contravened Data Protection Principle ("**DPP**") 3 under the Personal Data (Privacy) Ordinance ("**PDPO**") for the following reasons:<br><br>1. GDI massively collected and retained for its commercial exploitation public information, which was published by the Judiciary, Official Receiver's Office ("**ORO**") and the Companies Registry ("**Public Bodies**").<br><br>2. Such public information was published for various purposes, including to facilitate relevant persons to attend the designed court at the scheduled time, to ensure fair and open administration of hearings, handling of bankruptcy cases by the ORO and to enable the public to authenticate the identity of person holding out as officers of a company.<br><br>3. The disclosure of information through the App is not consistent with the purposes for which those data are published by the Public Bodies.<br><br>4. The use of the App exceeds the reasonable expectation of the data subjects on the use of their personal data by the Public Bodies, since the App:<br><br>• aggregated fragmented data from multiple sources to bring higher privacy risks;<br><br>• allowed sensitive personal data being accessed without the data subjects' knowledge;<br><br>• made it difficult to restrict further use of the data;<br><br>• did not ensure that the data were accurate, valid and comprehensive; and<br><br>• was detrimental to rehabilitation.<br><br>The Commissioner stressed that personal data collected from the public domain is not open to unrestricted use. A data subject does not relinquish his right to data privacy merely because he agrees to the disclosure of his personal data at a specific time and for a specific purpose. Under DPP3, personal data should only be used for the purposes for which they are collected or a directly related purpose, unless with the prescribed consent of the data subject.<br><br>The Commissioner discovered that GDI also provided litigation and bankruptcy data through channels other than the App. It has commenced a compliance check against GDI to ensure that parties concerned comply with the requirements under PDPO, but it refuses to comment on GDI's operation further before the compliance checks are completed. | The Commissioner served on GDI an enforcement notice, directing GDI to cease disclosing the litigation, bankruptcy and company directors' data held by it to the subscribers of the App.<br><br>GDI confirmed its compliance with the enforcement notice was in effect from 07 August 2013. |

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **24 October 2013** | **Hospital Authority** ("**HA**") | **<u>Key facts:</u>**<br><br>Hospital waste including used printer ribbon and shredded strips of medical appointment slips containing patients' data were found abandoned on the street outside a shredding factory which had been appointed as the waste disposal service provider of the HA (the "**Service Provider**"). HA had entered into a contract with the Service Provider ("**Contract**").<br><br>**<u>The Commissioner's findings:</u>**<br><br>Security measures (e.g. specifying the maximum width of shredding) are found in the Contract but they are only in relation to the processing of one category of wastes, not all of the wastes containing patients' personal data. HA and its hospitals are entitled to inspect the shredding process under the Contract, but HA had not monitored the inspections carried out by hospitals. There is no guideline or coordination between HA and hospitals as to the frequency, scope or reporting requirement for such inspections. HA had conducted infrequent inspections of the factory of the Service Provider and had identified key problems e.g. incomplete shredding of waste.<br><br>Under the Contract, HA is entitled to carry out audit to verify whether the Service Provider had complied with its contractual obligations and the requirements under PDPO. However, HA had not carried out any such audit.<br><br>The Commissioner concluded that HA had contravened DPP4 for having failed to take all reasonably practicable steps to ensure patients' personal data were protected against unauthorised or accidental access. | The Commissioner has served an enforcement notice on HA directing it to:<br><br>1. make reasonable endeavour to retrieve and destroy the abandoned hospital wastes identified in the incidents within 3 months of the enforcement notice;<br>2. review and revise the hospital wastes disposal process, and implement at the minimum the following improvement measures within 4 months of the enforcement notice:<br><br>• separate hospital wastes containing personal data into paper wastes and non-paper wastes;<br>• specify by contractual or other means how to safeguard used thermal ribbons and to ensure they are shredded in a manner which prevent the personal data contained therein from being readily recognised or recovered;<br>• ensure all paper wastes with personal data are treated at the highest security level;<br>• review and revise the Service Provider's monthly report format to enable meaningful and effective monitoring;<br>• conduct comprehensive audit to cover the whole waste disposal process;<br>• conduct inspections of hospitals and the Service Provider's shredding factory at least once annually<br>• assume a central monitoring role in the hospitals' inspection of the shredding factory; and promulgate to hospitals policies and guidelines in this regard. |

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **November 2013**[1] | Entity being complained:<br><br>**A government department**<br><br>(Note: no infringement found) | **<u>Key facts:</u>**<br><br>The Appellant submitted a Data Access Request ("DAR") Form to his former employer, a government department, for copies of his appraisal reports to seek new jobs. The government department provided copies of these reports to the Appellant but redacted the names, post titles and signatures of the appraisers. The Appellant was previously supplied with unedited copies of the reports but he had lost them. He complained to the Commissioner alleging that the government department failed to comply with his DAR.<br><br>**<u>The Commissioner's findings:</u>**<br><br>As the redacted names, post titles and signatures were not the personal data of the Appellant but were the personal data of the officers, the Commissioner concluded that the DAR had been fully complied with and decided not to issue any enforcement notice. | **<u>The AAB's decision:</u>**<br><br>The AAB followed the principle in *Wu Kit Ping v. Administrative Appeals Board, HCAL No. 60 of 2007*. A data subject was only entitled to access his personal data and not to every document in which a reference was made of him. The AAB found that the redaction was legitimate because:<br><br>1. The redacted data are not personal data of the Appellant so he has no right of access to them.<br><br>2. By virtue of section 20(2)(b) of the PDPO, a data user is excused from complying with a data access request to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of identifying particulars.<br><br>**The AAB upheld the Commissioner's decision and dismissed the appeal.** |

[1] This is appeal to the Administrative Appeal Board ("**AAB**") against the Commissioner's decision.

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **18 November 2013**[2] | Entity being complained:<br>**Housing Authority** (the "**Authority**")<br>(Note: complaint not pursued) | **Key facts:**<br>The Appellant had changed her name and requested the Authority to correct her name in their record. The Authority replied the Appellant that it was necessary to review her original identity document for verification before making the correction. The Appellant refused to produce her original identity document and complained to the Commissioner. | **The Commissioner's findings:**<br>The Appellant provided a copy of her HKID Card to the Authority. However, the photograph was covered by a symbol and the word "copy" was on the document. The Commissioner was of the view that it was prudent for the Authority to request for a review of the original HKID Card. As the Appellant refused to produce her original HKID Card, the Authority did not contravene DPP2(1) by not correcting the Appellant's name (DPP 2(1) provides that all practicable steps shall be taken to ensure the accuracy of personal data). The Commissioner decided not to pursue the complaint further.<br>**The AAB's decision:**<br>The AAB upheld the Commissioner's decision and dismissed the appeal. |

[2] This is appeal to the Administrative Appeal Board ("**AAB**") against the Commissioner's decision.

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **05 December 2013** | **California Fitness** ("**CF**") | **Key Facts:**<br><br>Complaints were made against the policies and procedures for membership application and renewal of CF, a fitness centre chain. CF collected its applicant's full date of birth (comprising year, month and date), Hong Kong Identity Card ("**HKID Card**") number, and copy of HKID Card or alternatively, the Mainland Travel Permit for Hong Kong Residents. CF is in possession of around 200,000 copies of HKID Card of current and former members.<br><br>**The Commissioner's findings:**<br><br>*Full Date of Birth:* CF claimed that collection of full date of birth was necessary to (1) establish the legal age of the applicant, and (2) design and promote its products and services to the members. The Commissioner considered that verification of age by examining the applicant's HKID Card on the spot and collection of the member's age range and month of birth would suffice for the two purposes. Therefore CF's collection of the member's year and date of birth was excessive and contravening the requirements of DPP 1(1) in the PDPO, which provides that collection of personal data must be necessary and not excessive for a lawful and relevant purpose of CF, i.e. membership application/renewal in this case.<br><br>*HKID Card Number:* The Commissioner accepts the collection of HKID Card number for inclusion in the membership agreement which entails significant rights and obligations of the members.<br><br>*Copy of Identity Card and Travel Permit:* CF claimed that collection of the copy of the identity documents was necessary to (1) ascertain members' legal names for legal proceedings, (2) verify membership income, and (3) support their staff remuneration system for reward of achievement of sales targets by deterring fake membership applications. The Commissioner considered that there are alternative measures to fulfil the above purposes effectively. Therefore CF's collection of the copy of identity documents was excessive and contravening the requirements of DPP 1(1). | The Commissioner served an **enforcement notice** on CF directing it to remedy and prevent any recurrence of the contravention. |

# Hungary

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **October 2013** | **A limited liability company** | The employee received a laptop from his employer for the performance of his work. Private use was allowed provided it did not hinder the efficiency of work. The employee was also a trade union member.<br><br>The managing director of the infringing entity requested the laptop from the employee in order to perform a system back-up for security reasons. The employee refused to hand over the laptop as it contained personal and trade union data and requested time to delete the data concerned. After deletion the employer restored the data deleted.<br><br>Later the managing director of the infringing entity disclosed printed photos to the employee (including his naked pictures, pictures of bank account, credit card data, family members, health data, list of trade union members). The managing director offered the employee that nobody will see these pictures if he signs a declaration that he is the one pictured on the photos. The employee refused to sign the declaration and later was dismissed with immediate effect.<br><br>The infringing entity claimed that the employee was only allowed to delete private data, however, according to the data recovered, he also tried to delete confidential company data. It was also claimed that the folders on the computer did not have titles.<br><br>Although the infringing entity had an IT policy in force, the monitoring of employee devices were not regulated therein.<br><br>The National Authority for Data Protection and Freedom of Information ("**Authority**") established that the data controller should have adequately regulated employee monitoring in its IT policy. By failing to do so, the data controller infringed the relevant provisions of the Privacy Act. | The Authority imposed a fine of HUF 1,500,000 (approx. **EUR 5,000**), prohibited the unlawful data processing, and ordered the infringing entity to regulate the monitoring electronic devices provided to employees and to refrain from restoring the data deleted from the employee's device. |

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **October 2013** | **Sanoma Media Budapest Zrt.** | On the recruiting webpage operated by Sanoma Media Budapest Zrt. anonymous vacancies were posted. When registered users applied for these positions they could not trace their personal data, did not know who would receive their application and they could not exercise their rights to data protection (i.e. did not receive information on data processing, could not protest against data processing, could not request the deletion of data).<br><br>The Authority established that consent from data subjects should have been obtained, however, data subjects did not even receive adequate information about data processing (i.e. the data controller, the term of data processing). | The Authority imposed a fine of HUF 200,000 (approx. **EUR 670**). |
| **October 2013** | **NETRIS Kft.** | The infringing entity operates a dating webpage. The Authority established that the data controller did not apply age restriction during the registration process, so children under the age of 16 could register without requiring the approval /consent of their guardian.<br><br>In addition, by completing the registration data subjects automatically consented to receiving newsletters, which does not fulfil the requirement of voluntary, unambiguous and informed consent.<br><br>In its privacy policy the infringing entity did not inform data subjects about their rights and remedies in connection with date processing.<br><br>The abovementioned conduct of the data controller infringed the relevant provisions of the Privacy Act, the Civil Code, the E-Commerce Act and the Advertising Act. | The Authority imposed a fine of HUF 450,000 (approx. **EUR 1,500**) and ordered the infringing entity to delete the unlawfully processed data or obtain the consent of the data subjects' guardians for the registration, to modify the existing practice relating to obtaining consents to send out newsletters in order to comply with privacy provisions and to modify its privacy policy in order to comply with statutory provisions. |

| Date | Infringing entity* | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **November 2013** | **Fővárosi Ásványvíz- és Üdítőipari Zrt. (the Hungarian subsidiary of PepsiCo)** | It was claimed that the infringing entity transferred date of birth, e-mail address and phone number to third parties and these data were publicly disclosed on the Internet.<br><br>The infringing entity started a promotional webpage, which was hacked by a Turkish hacker group and the personal data (incl. name, e-mail address, password, date of birth, phone number) of more than 50,000 users were stolen. The data stolen were disclosed on the Internet and were accessible for more than 9 months.<br><br>The Authority investigated whether the infringing entity complied with data protection rules on data security and rights of data subjects.<br><br>Although the infringing entity tried to mitigate the effects of the data breach and notified the data subjects, the Authority established that the infringing entity did not comply with the provision of the Privacy Act on data security as the hacker attack took place one year after the promotion had ended, the data processed were stored in database accessible from the Internet and even the UK based centre of the infringing entity found after a security control which took place during the promotion that there were some vulnerabilities. | The Authority imposed a fine of HUF 1,500,000 (approx. **EUR 5,000**). |

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

# Italy

| Date | Infringing entity | Details of infringement[3] | Sanction(s) imposed |
|---|---|---|---|
| **05 September 2013** | **Leon d'oro Shi e Shi di Shi Deshao e C. S.n.c.** | The company installed a CCTV system inside its building without posting any notice informing the data subjects. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 2,400**, by way of a reduced pecuniary administrative sanction. |
| **05 September 2013** | **Mr. Stefano Evangelista** | The owner of a restaurant installed a CCTV system, with cameras outside the restaurant, without posting a suitable and complete notice informing the data subjects. | **The Italian Data Protection Authority:**<br>Fined the owner of the restaurant **EUR 2,400**, by way of a reduced pecuniary administrative sanction. |
| **05 September 2013** | **CURTIPETRIZZILANDIA S.a.s. di Carrisi Francesco & C.** | The company collected basic personal data through an online reservation form asking information to book its services without providing adequate information. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 2,400**, by way of a reduced pecuniary administrative sanction. |
| **05 September 2013** | **Iniziative Commerciali S.r.l.** | The company collected basic personal data through an online reservation form asking information without providing adequate information. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 4,800**, by way of a reduced pecuniary administrative sanction. |
| **05 September 2013** | **Despar-Aspiag Service S.r.l.** | The company, a supermarket, installed 8 security cameras, inside and outside of its building, with a retention period of 5 days.<br>The 5 day retention period was significantly longer than the 24 hours authorised by the competent local labour office. | **The Italian Data Protection Authority:**<br>• declared the retention period of 5 days unlawful; and<br>• ordered the company to limit the retention period to 24 hours. |

[3] This table contains the most important cases examined in recent months by the Garante, without making reference to the several, as well as usual, claims made having regard to the exercise of the rights of the data subjects filed against banks and credit information companies.

| Date | Infringing entity | Details of infringement[3] | Sanction(s) imposed |
|---|---|---|---|
| **12 September 2013** | **Gruppo Nadine S.r.l.** | The company installed CCTV systems in four of its stores, without the prior agreement of the trade unions or the authorisation of the competent local labor office.<br><br>Furthermore, the notice posted by the cameras was insufficiently detailed (the identity of the data controller was omitted). | **The Italian Data Protection Authority:**<br>• Declared the processing of data unlawful<br>• Ordered the company to complete the procedures provided by art 4 l. no. 300/1970<br>• Ordered the company to amend the information notice according to article 13 of the Italian DP Code. |
| **12 September 2013** | **Store owned by Mr. Cheng Liangxiao** | The owner of a store installed a CCTV system inside the building without providing notice. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 2,400**, by way of a reduced pecuniary administrative sanction. |
| **12 September 2013** | **Comune di Mantova** | The Municipality of Mantova published population statistics on its website, which was in violation of the Italian DP Code.<br><br>The Italian DPA assessed that such information was never truly anonymous as it was possible to obtain information that identified the data subjects with a reasonable combination of variables. | **The Italian Data Protection Authority:**<br>Fined the municipality **EUR 10,000**, by way of pecuniary administrative sanction. |
| **12 September 2013** | **Azienda USL di Viterbo** | A hospital processed personal data without:<br>1. formally assigning its staff as persons in charge of the data processing;<br>2. providing written instructions on the processing; and<br>3. updating the security policy documents. | **The Italian Data Protection Authority:**<br>Fined the hospital with an amount of **EUR 10,000**, by way of pecuniary administrative sanction. |
| **12 September 2013** | **European Group Sae** | The company sent out unsolicited commercial communications by fax (where fax numbers were collected from third party databases), without prior notice and with no evidence of obtaining consent from the recipients. | **The Italian Data Protection Authority:**<br>Fined the company with an amount of **EUR 12,800**, by way of a reduced pecuniary administrative sanction. |

| Date | Infringing entity | Details of infringement[3] | Sanction(s) imposed |
|---|---|---|---|
| **September 12, 2013** | **Topway S.r.l.** | The company installed a CCTV system to protect its store without the prior agreement of the trade unions or the authorisation of the competent local labour office. | **The Italian Data Protection Authority:**<br>• Declared the processing of data unlawful;<br>• Ordered the company to complete the procedures provided by relevant legislation. |
| **September 19, 2013** | **Cooperativa di servizi Aggrego** | The company sent out unsolicited commercial communications by fax (where fax numbers were collected from third party databases), without prior notice and with no evidence of obtaining consent from the recipients. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 6,400**, by way of pecuniary administrative sanction. |

| Date | Infringing entity | Details of infringement[3] | Sanction(s) imposed |
|---|---|---|---|
| **03 October 2013**<br>**(two separate decisions)** | **Lycamobile S.r.l.** | The company failed to produce documents and information requested by the Italian DPA during an inspection, following which it was fined EUR 20,000, by way of pecuniary administrative sanction.<br>Following further investigations, it was found that the company violated several provisions contained in the general decision found in "Security In Telephone And Internet Traffic Data" (17 January 2008), including failure to:<br>1. implement specific computerised authentication systems;<br>2. have in place separate functions among those who have access to data; and<br>3. implement separate IT systems for different types of data.<br>Furthermore, the company:<br>1. retained both telephone and internet traffic data for 24 months where the prescribed retention period is 12 months;<br>2. used traffic data for marketing purposes, which was prohibited by the aforementioned general decision;<br>3. processed personal data without providing any adequate lawful information; and<br>4. did not designate its IT service provider as the data processor. | **The Italian Data Protection Authority:**<br>• Declared the processing of personal data unlawful and prohibited any further use; and<br>• Ordered the company to take measures to comply with the security provisions as set out by the general decision of the Italian DPA. |

| Date | Infringing entity | Details of infringement[3] | Sanction(s) imposed |
|---|---|---|---|
| **03 October 2013** | **Comune di Canicattì** | The Municipality of Canicattì published on its website, personal data (including health data) of some citizens in excess to those required by the applicable laws on transparency of the Public Administration, and in violation of the Italian DP Code. | **The Italian Data Protection Authority:**<br>• Prohibited the municipality of Canicattì from any further dissemination and publication of sensitive and excessive personal data via the Internet;<br>•Ordered the municipality to take any necessary step to have the major search engines (e.g. Google) remove the copies of the documents from the Internet. |
| **03 October 2013** | **Forum Sport Center, società sportiva dilettantistica S.r.l.** | The company collected personal data on a registration form without giving a complete information notice, and also installed a CCTV system without posting notice. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 8,400**, by way of a reduced pecuniary administrative sanction. |
| **03 October 2013** | **Telecom Italia S.p.a.** | The company made commercial communications by telephone to one of its clients, who had previously opted-out of marketing communications, to inform him of the possibility to apply to the opt-out register.<br>The company therefore processed personal data without prior and specific consent from the recipient. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 80,000**, by way of pecuniary administrative sanction. |
| **10 October 2013** | **TeleTu S.p.a.** | The company made several promotional communications by telephone to one of its clients, without obtaining prior and specific consent from the recipient. | **The Italian Data Protection Authority:**<br>Fined the company **EUR 60.000**, by way of pecuniary administrative sanction. |

| Date | Infringing entity | Details of infringement[3] | Sanction(s) imposed |
|---|---|---|---|
| **10 October 2013** | **Santander Consumer Bank S.p.a.** | The bank implemented a procedure for the recollection of financing credits through pre-recorded telephone messages, without the intervention of an operator and without a procedure for identifying the debtor over the phone.<br><br>With its general decision "Debt Collection and Processing of Personal Data" (November 30 2005) the Italian DPA had specifically declared that the use of pre-recorded telephone messages without an operator's intervention to recollect credit, is an unlawful processing operation, since there is the risk that third parties may become aware of the situation of the debtor. | **The Italian Data Protection Authority:**<br><br>• Declared the use of pre-recorded telephone messages without an operator unlawful, prohibiting any further use; and<br><br>• Ordered the bank to adopt any technical steps (such as an authentication procedure) to ensure that only the debtor could receive the pre-recorded telephone messages. |
| **30 October 2013** | **Comune di Bolzano** | The Municipality of Bolzano published on its website, a document revealing the health data of a member of the Board, in violation of the Italian DP Code. | **The Italian Data Protection Authority:**<br><br>Fined the municipality **EUR 10,000**, by way of pecuniary administrative sanction. |
| **07 November 2013** | **Comune di Nogara** | The Municipality of Nogara, through a public reading during an official meeting and the publishing of the minutes of the meeting on its website, disseminated information revealing health data of a citizen, in violation of the Italian DP Code. | **The Italian Data Protection Authority:**<br><br>Fined the municipality **EUR 10,000**, by way of pecuniary administrative sanction. |
| **18 December 2013** | **Google Inc.** | The Italian DPA sanctioned Google for failing to provide adequate information to data subjects while collecting data for its Streetview service. | **The Italian Data Protection Authority:**<br><br>Fined Google Inc **Eur 1,000,000**, by way of a pecuniary administrative sanction. |

# Poland

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **Court Judgments** | | | |
| **13 August 2013**<br><br>(II SA/Wa 149/13) | **Company** | An individual requested the Inspector General for the Protection of Personal Data ("**GIODO**") to order the Company to cease processing the individual's biographic note. The note was made available to the public through the website run by the Company.<br><br>GIODO stated that the Company is not the data controller because it does not possess the biographic note and cannot edit or delete the data. The Company only made the note available through its website *via* an embedded link to an Internet encyclopaedia. | The individual filed a complaint against GIODO's decision to the Regional Administrative Court.<br><br>The Court upheld the decision repeating GIODO's arguments. |
| **21 August 2013**<br><br>(I OSK 1666/12) | **Agora S.A. (publishing company)** | Upon Agora's request, GIODO ordered Company A to reveal the e-mail addresses and IP numbers of the authors of 36 entries that allegedly infringed Agora's personal rights.<br><br>Company A filed a complaint against GIODO's decision to the Regional Administrative Court. | The court stated that the Personal Data Protection Act (the "**Act**") does not apply to this case, but rather the Act on Rendering Electronic Services, which does not allow personal data to be revealed to entities other than competent public authorities.<br><br>The Supreme Administrative Court accepted an appeal arguing that users' personal data should be disclosed if it is necessary to protect personal rights and reputation. The provisions of the Act on Rendering Electronic Services are not against disclosing personal data to private entities. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **05 September 2013**<br><br>(II SA/Wa 735/13) | **Television Company** | An individual requested GIODO to order the Television Company to disclose journalists' addresses and their ID numbers (PESEL). The individual had already filed a lawsuit against the above-mentioned journalists due to the alleged infringement of personal rights. However, the proceedings before the civil court were suspended due to the unavailability of the journalists' addresses.<br><br>GIODO ordered the Television Company to disclose the journalists' addresses but not PESEL numbers. GIODO emphasised that the right to privacy is not absolute and acknowledged that only addresses (not PESEL numbers) are necessary to file a lawsuit under the Civil Proceedings Code.<br><br>The Television Company filed a complaint to the Regional Administrative Court against GIODO's decision. | The court upheld the decision and agreed with GIODO's reasoning. In the justification it was stated that the journalists' personal data cannot be disclosed only if the journalist marked a broadcast with her/his pseudonym and the journalist's anonymity is protected by the provisions of the Press Act.<br><br>If journalists marked the broadcast with their names, they became liable towards third parties for its content. Therefore there are no limitations to disclose the personal data of the journalists. |
| **05 September 2013**<br><br>(II SA/Wa 764/13) | **Court** | The Court (a controller of employees' data) requested a trade union to provide a list of the employees that would be represented by the trade union in case their contracts were terminated. As a result, the trade union filed a complaint to GIODO.<br><br>GIODO stated that the Court infringed the Act. The Court cannot request a list of protected employees since such information can only be revealed during consultations regarding the particular employee's case.<br><br>The Court Administrator filed a complaint to the Regional Administrative Court against GIODO's decision. | The court revoked GIODO's decision but explicitly stated that, under the Trade Union Act and the Labour Code, the employer can acquire personal data of its employees protected by the trade union only in particular cases.<br><br>The employer can only acquire employees' personal data upon a factual basis. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **08 October 2013**<br><br>(II SA/Wa 254/13) | **Television Company** | An individual requested the Television Company to disclose the addresses of journalists that have allegedly infringed personal rights with a program broadcast. The request remained unanswered.<br><br>GIODO ordered the Television Company to disclose the journalists' personal data since the individual authenticated that the journalists may have violated the personal rights and freedoms of the data subject and that the requested data are necessary to initiate court proceedings. | The Television Company filed a complaint to the Regional Administrative Court against GIODO's decision.<br><br>The court ordered GIODO to re-examine the case and argued that an intention to file a lawsuit is insufficient to order the revealing of personal data. The individual should have filed the lawsuit prior to their request. |
| **08 October 2013**<br><br>(II SA/Wa 977/13) | **A Municipal Council** | An individual requested the Municipal Council to provide information about processing personal data in the form of video surveillance. The Municipality Council informed that video recording is outside the scope of the Act, because it does not constitute a personal data filling system and video surveillance is not recorded.<br><br>GIODO dismissed the case stating that the Municipality Council has already fulfilled its information obligation towards the individual. The decision was based exclusively on the mayor's testimony.<br><br>The individual filed a complaint to the Regional Administrative Court. | The court revoked GIODO's decision stating that GIODO is obliged to ensure the compliance of data processing under the provisions of the Act.<br><br>GIODO should have therefore clarified the circumstances of the case and carried out an in-depth clarification regarding the individual's case. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **18 October 2013**<br>(I OSK 1487/12)<br><br>Similarly:<br>**18 October 2013**<br>(I OSK 129/13) | **A Roman Catholic parish** | An individual filed an official letter comprising a declaration of exiting the Roman Catholic Church and a request to make a correction to the baptism certificate. The parish replied that the individual is no longer a parishioner but, pursuant to Canon law, the apostasy declaration has to be submitted to the parish attended.<br><br>GIODO dismissed the case and refused to issue a decision since the Roman Catholic Church is an independent religious authority. | The individual filed a complaint to the Regional Administrative Court against GIODO's decision arguing that GIODO is obliged to issue a decision in the case directly based on the Directive 95/46/EC, because the Act unlawfully excludes the Roman Catholic Church from GIODO's competency.<br><br>The court upheld GIODO's decision.<br><br>The individual then filed an appeal against the first instance judgment to the Supreme Administrative Court.<br><br>The Supreme Administrative Court ordered the case to be re-examined arguing that the Roman Catholic Church is autonomous, but not independent from acts of the state, and the Polish constitution. Unless matters have been exclusively assigned to the Roman Catholic Church, the acts have to be applied; hence, GIODO cannot refuse to issue a decision. |
| **19 November 2013**<br><br>(II SA/Wa 1241/13) | **Company R.** | An individual requested GIODO to order Company R. to cease processing their personal data that was used to compose and submit offers regarding stock buyouts to the individual.<br><br>GIODO rejected the request, indicating that the processing of the individual's personal data was performed in compliance with the Act since Company R. legally acquired the personal data through the publicly accessible National Court Register in order to perform its legitimate interest, in particular, direct marketing.<br><br>The individual then requested GIODO to re-examine the case. GIODO ordered Company R. to fulfil the information obligations towards the individual since Company R. became the data controller by acquiring personal data indirectly, through the National Court Register. GIODO dismissed the complaint in the remaining scope. | Company R. filed a complaint the Regional Administrative Court against GIODO's decision.<br><br>The court upheld GIODO's decision and stated that Company R. was obliged to provide the data subject to the information immediately, at the latest when submitting the offer. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **19 November 2013**<br><br>II/SA/Wa 666/13 | **Company** | The Company commissioned work to the research centre consisting of separating DNA from biological samples. The Company requested GIODO to register the personal data filing system comprising the data separated from biological samples.<br><br>GIODO refused to register the personal data filing system because the Company did not conclude an authorisation agreement for personal data processing with the research centre. Storing DNA samples constitutes processing sensitive personal data. If each DNA sample is marked with a special code, the research centre can identify individuals. | GIODO's decision was appealed before the Regional Administrative Court.<br><br>The court upheld the decision repeating GIODO's argument. |
| **Decisions of the Inspector General for the Protection of Personal Data** | | | |
| **23 August 2013**<br><br>(DOLiS/DEC-859/13) | **Bank** | The Bank, in which a trade union has its bank account, stopped providing data regarding members' payments. The Bank refused to disclose the data requested by the trade union, following which the trade union requested GIODO to order the Bank to disclose the data. | GIODO ordered the Bank to disclose the Bank's clients' names, surnames and amounts of deductions for the trade union, pursuant to the Trade Union Act.<br><br>GIODO stated that the above-mentioned data are necessary to conduct union activity, because the trade union's members are obliged to pay monthly fees, which if not paid can result in cancelled memberships. |
| **29 August 2013**<br><br>(DOLiS/DEC-880/13) | **Company U.** | An individual requested GIODO to order Company U. to disclose the names, surnames and addresses of users that use listed IP numbers. The individual stated that the users have allegedly infringed their exclusive rights to translate and publish works in Poland. The individual stated that they intend to file a lawsuit against those people. | GIODO dismissed the application arguing that the requested data are covered by telecommunication secrecy and cannot be revealed under the Act because the scope of protection provided by telecommunication secrecy is wider than that of the Act. |
| **29 August 2013**<br><br>(DOLiS/DEC-377/12/27589,27593) | **The Municipal Council** | An individual requested GIODO to order the Municipal Council to cease processing his/her private telephone number. The individual had used the number for work purposes in the Council. The Council stated that it does not process their data. However, the telephone number (personal data) was retained on documents that have to be kept for two years. | GIODO dismissed the application arguing that the Municipal Council processes the individual's personal data for the purpose of performing the obligations resulting from a legal provision. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **Protection of Personal Data infringement** | | | |
| **17 December 2013**<br><br>(Press release) | **Individuals** | Three persons had allegedly stolen personal data of a major telecommunication provider's clients (Orange S.A.). They offered them for sale over the Internet and were caught during a sale attempt. | The Prosecution Office has initiated a criminal investigation into the case. |

# Spain

| Total number of resolutions | Classification of matters to which infringements refer | Number of resolutions |
|---|---|---|
| **186 resolutions** | Improper inclusion of personal data in a defaulters list | **21** |
| | Processing of personal data without consent | **57** |
| | Commercial communications | **14** |
| | Video surveillance | **9** |
| | Other resolutions (data inaccuracy; obligation to secrecy; data security; disclosure of personal data without consent; data subject's rights; information right when processing personal data). | **85** |

| Some highlighted resolutions | | | |
|---|---|---|---|
| **Date** | **Infringing entity** | **Details of infringement** | **Sanction(s) imposed** |
| **20 September 2013** | **Directo a Casa Venta Directa, S.L.** | Continuous mailing of commercial communications despite repeated requests to object to receiving commercial communications. Furthermore, other clients' email addresses also appear in the email | The SPDA imposed two fines: one of **EUR 1,200** due to the infringement of Article 22.1 LSSI (commercial communications), and the other one of **EUR 1,000** due to the infringement of Article 10 LOPD (obligation to secrecy). |
| **30 September 2013** | **Vodafone España, S.A.** | Undue inclusion of an uncertain debt (was pending a litigation) in a defaulters list. Also, on the debt claim, Vodafone had not told the alleged debtor about their possible inclusion in a list of defaulters. | The SPDA imposed a fine of **EUR 50,000** due to the infringement of Article 29.4 LOPD (veracity of the data given to lists of defaulters). |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **03 October 2013** | **EMMASA-Empresa Mixta de Aguas de Santa Cruz de Tenerife, S.A.** | Several resumes of EMMASA's candidates could be accessed by Google due to the fact that, according to the SPDA, appropriate security measures were not adopted by EMMASA. | The SPDA imposed a fine of **EUR 20,000** due to the infringement of Article 9 LOPD (security of data). |
| **29 October 2013** | **Telefónica España, S.A.U.** | Undue disclosure of client personal data to another company to be published in a record of subscribers when the client expressly prohibited such. | The SPDA imposed a fine of **EUR 15,000** due to the infringement of Article 11.1 of LOPD (disclosure of personal data to a third party). |
| **06 November 2013** | **Vodafone España, S.A.** | Vodafone registered four telephone lines under the name of a person judicially declared incapable. In addition, they improperly registered him on a list of defaulters. | The SPDA imposed two fines: one of **EUR 60,000** due to the infringement of Article 4.3 LOPD (accuracy and veracity of personal data), and the other of **EUR 60,000** due to the infringement of Article 6.1 LOPD (need for previous consent). |

# Sweden

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **09 September 2013** | Utbildnings- och arbetsmarknadsnämnden i Sollentuna Kommun<br>*(The Education and Employment Board of Sollentuna municipality)*<br>(the "**Municipality**") | Students and employees at a school within the Municipality used the cloud computing service *Google Apps for Education* for which the Municipality was the data controller. Hence, the Municipality was responsible for processing personal data in such cloud computing service.<br>The Swedish Data Inspection Board found that the agreement between the parties did not include sufficient information regarding data processing activities, security measures, or data transfers. | The Data Inspection Board (the "**DIB**") ordered the Municipality to:<br>• Cease using the cloud computing service *or*<br>• Take measures to enter into a processor agreement with the Service provider drafted in accordance with the provisions set forth in the Swedish Personal Data Act (the "**PDA**"). |
| **09 October 2013** | **Gotlands tingsrätt**<br>(*Gotland District Court*)<br>(the "**Court**") | The Court published lists of the various cases being subject to trial at the Court, on their website. Such lists contained names of persons who were parties to the cases that had not yet been decided. Hence, the Court published *inter alia* names of suspects in criminal cases. | The Administrative Court of Appeal in Stockholm granted leave to appeal and tried the case. The Administrative Court of Appeal in Stockholm came to the same conclusion as the DIB and the Administrative Court in Stockholm previously had done.<br>The publication of case lists on the Court's website did not constitute the processing of structured information. Consequently, the rules regarding processing of personal data did not apply. Based on the regulation regarding misuse set forth in the PDA Section 5a, the publication of case lists was found to constitute an aggrievement. Therefore, the publication was prohibited by the Administrative Court of Appeal. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **14 October 2013** | **Styrelsen för Karolinska universitetssjukhuset**<br>(*The Board of Karolinska University Hospital*)<br>(the "**Hospital**") | The Hospital processed personal data when making debit card transactions. The information that was sent to the payment service provider through the debit card transaction contained data regarding *inter alia* that payment was made at the hospital, at which ward payment was made (e.g. the maternity ward), date, time, civic registration number, care giver, costs and account number. Such processing was investigated by the DIB. | The DIB found that the Hospital processed personal data in breach of the PDA, by disclosing personal data that was not adequate or relevant for the purpose and by disclosing excessive data (i.e. more data than necessary to make the payment).<br>The DIB required the Hospital to immediately cease the disclosure of such personal data to the payment service provider. |
| **29 October 2013** | **Socialdemokraterna**<br>(*The Swedish Social Democratic Party*)<br>(the "**Party**") | The Party is a political organisation.<br>According to Section 17 of the PDA, a political organization is allowed to process sensitive personal data. Such data may however only be disclosed to a third party if the data subject has given his or her explicit consent to such disclosure.<br>The DIB investigated the Party's processing of personal data and found that the Party disclosed sensitive personal data (i.e. data regarding political opinions) about their members without any explicit consent to do so, to a subsidiary (a third party) of a company owned by the Party (the "**Subsidiary**").<br>The Subsidiary conducted *inter alia* lotteries, with the purpose of supporting the Party financially. The Party disclosed sensitive personal data of their members to the Subsidiary, in order for the Subsidiary to contact the members of the Party with the purpose of selling lottery tickets to them. | The Administrative Court of Appeal in Stockholm (the "**Court**") tried the case and affirmed the decision from the DIB.<br>The DIB had found that the Party had processed sensitive personal data in breach of Section 17 of the PDA. The DIB ordered the Party to either (i) cease the disclosure of sensitive personal data to the Subsidiary *or* (ii) set up routines ensuring that such sensitive personal data was only processed subject to the members' consent to such use.<br>The Party argued that the Subsidiary was the Party's data processor, and therefore consent was not necessary. The Court stated that the purpose of the Subsidiary's processing of the sensitive personal data was to make the members of the Party their customers. The purpose of the processing in the Subsidiary could therefore not be considered to be the same purpose that the Party had for the processing of the sensitive personal data. The Subsidiary's processing of the sensitive personal data could not be considered to be made on the behalf of the Party. Furthermore, the Court stated, that the fact that an agreement between the Party and the Subsidiary was entered into, in which it was stated that the Subsidiary was the data processor of the Party did not change the situation (i.e. that the Subsidiary could not be considered to be the data processor in this respect). The Court affirmed that the Party's disclosure of data was in breach of Section 17 of the PDA. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **18 November 2013** | **Axfood Sverige AB division Dagab**<br>("**Axfood**") | Axfood conducts retail and wholesale of food in Sweden.<br>Axfood wanted to use a service in their vehicles, based on a technology that makes the drivers' drive according to the speed limits. Such technology implied that it was immediately displayed at a screen placed in the vehicle if the driver was speed driving or not. The information on the screen would be continuously updated as long as the driver was driving the vehicle.<br>Therefore, Axfood applied for an exemption from the prohibition to process data regarding criminal offences under Section 21 of the PDA.<br>The supplier's intention was to save consolidated data regarding the driver's average speed and how often such drivers had been speed driving, and provide Axfood with reports of such data. Axfood intended to use the reports solely for the purpose of promoting traffic safety to the drivers. | The DIB found that Axfood shall have the right to process personal data regarding such criminal offences, subject to the following conditions:<br>• Ensuring that the surveillance is consistent with good practice on the labor market;<br>• Only using the data to induce a driver to drive in accordance with the current speed limits;<br>• Saving the data for a maximum of three (3) months;<br>• Developing proportionate and documented routines for how the controls of and the feedbacks to the drivers shall be made, as well as distinct data processing rules for the persons that will have access to the data;<br>• Informing the drivers of how the controls and the feedback to the driver will be carried out and informing the drivers of the fact that the reports in some cases can be based on inaccurate information;<br>• Limiting the access to the data through an access control system;<br>• Introducing a logging procedure for the systems when personal data is accessed, and developing log surveillance routines;<br>• Encrypting any personal data that is transmitted over the internet. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **26 November 2013** | **Polismyndigheten Gotland**<br>(*The police authority Gotland*)<br>(the "**Police**") | The DIB investigated the Police's processing of personal data. During the DIB's investigation, several deficiencies were identified, including the following:<br>1. The Police have appointed a data protection officer in accordance with the Police Data Act. Such officer is obligated to maintain a register of all personal data processing that is conducted by the Police. Such existing register had not been updated after the implementation of the new Police Data Act;<br>2. Investigations handled in the Police's computer systems were named by use of personal data (i.e. an investigation file could have the name or civic number of a suspected person);<br>3. No inspections had been performed regarding who had access to filed personal data and who needed that kind of access;<br>4. Furthermore, the Police had no routines to ensure the quality of the data before such data was published on their internal information site. Moreover, there were no routines to ensure that data was deleted from such site when the data was not relevant anymore. | The DIB ordered the Police to take several measures, including:<br>• Provide the data protection officer with the data needed to enable such person to pursue an updated register over the processes of personal data conducted by the Police;<br>• Introduce routines to ensure that an added indication of secrecy in the national registration register be noticed in the systems used by the Police and registered in the systems at the latest in conjunction with the final report in the matter;<br>• Develop written routines containing security measures in reference to the processing of personal data on mobile devices;<br>• Introduce a logging procedure for the systems and to develop log surveillance routines to detect and prosecute unauthorized access to personal data in the systems;<br>• Review its routines for limiting the access to filed personal data, so that the access to filed personal data is limited to what every employee needs in order to fulfill their duties;<br>The DIB also stated that the Police shall submit an action plan to the DIB containing a report of the measures that the Police has taken in order to fulfill the above stated measures. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **06 December 2013** | **Krafman AB**<br>(the "**Company**") | The Company was one of the parties in a court trial, which had previously been decided. Thereafter, the Company had uploaded the judgment of such case on their website. The uploaded document contained the name and address to the adverse party, which was a natural person. | The Supreme Court held that such uploading of the document was processing of personal data. However, it was not a question of any processing where the information was structured in a manner that significantly facilitated the search or compilation of personal data. Therefore, the uploading did not constitute such processing of personal data which is subjected to the processing rules set forth in the PDA. However, the processing implied violation of the integrity of the named person, and therefore damages shall be paid in accordance with the PDA, Section 48. |

# Switzerland

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **25 November 2013** | **Unknown** | A bank experienced a large data leak, where an IT employee was able to steal a large quantity of personal and financial data regarding the bank's clients. According to the FINMA, the Swiss supervisory authority, the bank should have had additional measures to prevent the leak from happening. In its decision, the FINMA noted that confidential clients' data were inappropriately disseminated, with confidential data sometimes being classified as non-confidential and stored on less secure IT systems. | The FINMA issued a formal reprimand against the bank and noted that it took important additional measures to prevent further leaks from happening. |

# United Kingdom

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **25 September 2013** | **Jennifer Addo (former Barclays Bank employee)** | A former Barclays Bank employee was fined after illegally accessing the details of a customer's account.<br><br>The employee, Jennifer Addo passed on the account holder's personal information to the customer's former partner, who was a friend of the Ms Addo's.<br><br>An investigation followed after the account holder reported the disclosure to Barclays; and it was discovered that Ms Addo had illegally accessed the customer's details on 22 occasions between 10 May 2011 and 8 August 2011. This was despite Barclays informing its staff that they should not access customers' accounts unless required.<br><br>When interviewed by her employer, Addo confirmed that she was aware that the complainant's details should not have been accessed, but still decided to look at the complainant's file and pass information to her friend. Ms Addo failed to respond to the ICO's enquiries leading up to today's prosecution.<br><br>Ms. Addo's employment was terminated once the investigation was underway.<br><br>Following last month's similar incident in the case of a probation officer, this again raises the question of whether stricter penalties are required, as opposed to the current "fine only" approach. | **Prosecution under section 55 of the Data Protection Act and a fine of £2,990 for 23 offences as well as a £120 victim surcharge and £250 prosecution costs.** |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **26 September 2013** | **Jala Transport Limited** | Jala Transport, a small money-lending business lost a hard drive containing financial details relating to all of their 250 customers.<br><br>The stolen hard drive was password protected, but crucially not encrypted, and included details of the customers' name, date of birth, address, the identity documents used to support the loan application and details of the payments made.<br><br>During its summary, the ICO recognised the fact that the loss could amount to substantial damage and distress; however, it took into account the limited financial resources of the business, as well as the fact that the data breach was voluntarily reported. The Monetary Penalty was therefore reduced from £70,000 to £5,000.<br><br>Following this incident, the ICO reiterated the importance of encrypting data files for businesses of all sizes. | **Monetary Penalty of £5,000** |

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

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

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

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **18 October 2013** | **Panasonic UK** | Theft of an unencrypted laptop containing personal data relating to 970 individuals who had hospitality events organised by Panasonic UK including names, passport details, addresses and contact details. | **Undertaking imposed upon Panasonic UK to:**<br>• Put in place adequate contracts and checks to ensure that data controllers are capable of, and are continuing to, comply with the seventh data protection principle; and<br>• Ensure that personal data collected for a specified, valid purpose is not held for longer than is necessary for that purpose. |
| **22 October 2013** | **Ministry of Justice** | Three emails containing sensitive information of all of the inmates serving at HMP Cardiff were accidentally sent to three of the inmates' families between 4 – 2 August 2011. Each email included an attachment containing a spreadsheet including the names, ethnicity, addresses, date of birth, details of physical marks including tattoos, sentence length, release dates and coded details of the offences carried out by all of the prison's 1,182 inmates. Six of the prisoners had sex offence information recorded against them.<br><br>An internal investigation conducted by the Prison revealed that prior to the 2 August 2011 notification by one of the families, the data controller had not been aware that the unauthorised disclosures had occurred. | **Monetary Penalty of £140,000** |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **29 October 2013** | **North East Lincolnshire Council** | A special education needs teacher working for the data controller lost an unencrypted USB memory stick containing the sensitive personal data of 286 children. The memory stick was never recovered.<br><br>The children were aged between 5 and 16 years and the memory stick held data such as: mental and physical disabilities, specific teaching strategies required for a particular child, date of birth, home address and ' home-life' which included financial matters and family dynamics.<br><br>The ICO found that the loss of this data was likely to lead to the ill-health of those concerned; either through disclosure or a break in the services they were receiving. The potential damage and distress to data subjects, who were deemed 'vulnerable' and their families, was held to be 'substantial'. | **Monetary Penalty of £80,000** |
| **01 November 2013** | **Mansfield District Council** | The ICO conducted a follow-up review of Mansfield District Council's (**MDC**) actions following its undertaking of 17 January 2013. The ICO concluded that MDC had taken appropriate steps and put plans in place to address the requirements of the undertaking and mitigate the risk highlighted. | **No further action by MDC required.** |
| **01 November 2013** | **Health and Care Professions Council** | The ICO conducted a review of the Health and Care Professions Council (the "**Council**") in relation to the undertaking it signed in July 2013. The ICO found that the Council has or is taking appropriate steps to address the requirements of the undertaking. | **No further action by the Council required.** |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **20 November 2013** | **ICU Investigations Limited** | The men behind private investigation company "ICU Investigations Ltd" were found guilty of conspiring to unlawfully obtain or access personal data, a criminal offence under section 55 of the Data Protection Act 1998.<br><br>ICU Investigations Ltd worked on behalf of clients such as Allianz Insurance PLC, Brighton & Hove Council and Leeds Building Society, to trace individuals, primarily for the purpose of debt recovery. The court found that the company had tricked organisations such as utilities companies and TV licensing into revealing personal data. The ICO investigation found approximately 2,000 separate offences between 2009 and 2010.<br><br>Five employees had previously pleaded guilty to the charges and the company was also found guilty as a separate defendant. The ICO found no evidence of criminality by any of ICU Investigations Ltd's clients, who were found to be unaware of the fact that the data had been obtained by illegal means. | **Following a sentencing hearing on 24 January 2014, Adrian Stanton, who ran ICU Investigations Limited with Barry Spencer, was fined a total of £7500 and £6107 prosecution costs.**<br><br>**The ICO awaits the sentencing of Mr Spencer and ICU Investigations Ltd - which will be sentenced as a separate defendant - at a confiscation hearing on 04 April 2014.**<br><br>**Five employees of the company who had previously pleaded guilty to the same offence were also sentenced, with fines ranging from £1000 to £4000, not including prosecution costs.** |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **21 November 2013** | **Great Ormond Street Hospital for Children NHS Foundation Trust** | The ICO was informed of four separate incidents over 18 months where letters containing sensitive medical information was sent to the wrong addresses.<br><br>In the majority of the cases, the letters had been sent by temporary member of staff, who were exempt from data protection training.<br><br>Furthermore, it was found that failure to attend data protection training was not followed up in any way.<br><br>**The ICO has used this case to highlight the importance of organisations providing adequate data protection training to temporary and agency workers in roles which involve the day-to-day handling of personal data.** | **Undertaking imposed upon Great Ormond Street Hospital for Children NHS Foundation Trust to ensure that:**<br><br>• temporary or bank staff are provided with sufficient data protection training before they carry out work that involves regular contact with personal data, especially sensitive personal data;<br><br>• such training is fully monitored, and attendance is enforced where necessary;<br><br>• sufficient processes are put in place to ensure medical records and referral letters are sent to the correct address, and that practical guidance on these processes are communicated to all staff and;<br><br>• they implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **22 November 2013** | **Foyle Women's Aid** | The ICO conducted a review of the actions taken by Foyle Women's Aid in relation to the undertaking it signed in August 2013. The ICO found that the Foyle Women's Aid is taking appropriate steps to address the requirements of the undertaking. | **Further steps required under the Undertaking:**<br>• Data Protection training should be completed by the end of November 2013 as planned.<br>• Encryption software should be installed on all laptops, iPads and any other mobile devices used by staff.<br>• Procedural guidance should be introduced for staff to follow in relation to the secure use of mobile devices, as planned.<br>• The access restriction software training which is currently scheduled for 2014 should be completed by all relevant staff prior to its implementation.<br>• The contract with the external shredding company should contain appropriate security clauses and checks on the company's security procedures should be conducted annually. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **22 November 2013** | **Better Together** | Ahead of next year's Scottish Referendum vote, campaign group "Better Together" sent 300,000 messages to individuals in Scotland urging them to complete a survey confirming how they intended to vote.<br><br>The messages were sent out by a third party marketing company during March and April 2013. On both occasions, the campaign group failed to check whether the recipients had provided their consent to be contacted, believing that the consent had been obtained by another company working on their behalf.<br><br>Better Together agreed to sign an undertaking to comply with the Privacy and Electronic Communications Regulations.<br><br>**The ICO, which received 61 complaints following Better Together's actions, used this case to remind Scottish referendum campaign groups that they must comply with electronic marketing rules ahead of next year's vote.** | **Undertaking imposed stating that Better Together must neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail to individual subscribers unless the recipient of the electronic mail has previously notified Better Together that they consent.** |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **26 November 2013** | **Royal Borough of Windsor and Maidenhead** | A report containing the details of 257 individual employees, was published on a general section of the data controller's intranet, as opposed to a restricted section, as intended.<br><br>Although no sensitive personal data was included, and the data could only be accessed by the data controller's employees through the intranet, it was found that there were no mandatory data protection training requirements for staff handling data. Furthermore, the ICO found that the data controller's policies and procedures on the handling of personal data were incomplete. | **Undertaking imposed upon Royal Borough of Windsor and Maidenhead to ensure that:**<br><br>• they will review and revise policies and procedures for the handling and use of personal data, especially in the area of information security, and bring these into operation by no later than 31 December 2013;<br><br>• all staff shall be made aware of the policies and procedures by no later than 31 December 2013;<br><br>• from 31 December 2013, all staff whose roles involve access to personal data shall be trained in data protection and the data controller's policies and procedures on commencing their employment. All existing staff whole roles involve access to personal data shall receive such training no later than 31 December 2013. Such training shall be refreshed and updated regularly thereafter for all relevant staff, at intervals not exceeding two years;<br><br>• compliance with policies on data protection and training requirements shall be appropriately and regularly monitored and enforced; and<br><br>• they 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. |

| Date | Infringing entity | Details of infringement | Sanction(s) imposed |
|---|---|---|---|
| **03 December 2013** | **GP Surgery Manager** | During a review of the surgery manager's attendance file, it was discovered that he had accessed patients' records on 2023 occasions between August 2009 and October 2010. As the former surgery manager, Mr Tennison was only required to access the records on three occasions under the remit of his role, and having received adequate data protection training, was well aware of his unlawful behaviour. | **£996 fine and order to pay a £99 victim surcharge and £250 prosecution costs.** |
| **16 December 2013** | **First Financial (UK) Limited** | First Financial offers payday loans. ICO received complaints from over 4,000 people about texts sent without consent during two months in 2013. First Financial sent the texts using unregistered SIM cards to try and avoid detection.<br><br>The monetary penalty notice emphasises the disturbing impact of the texts viz. they were often sent in the early hours; some were on numbers only used for contact with elderly relatives; roaming charges were incurred etc.<br><br>The ICO relied on a Direct Marketing Association article to suggest that only 3% of people receiving spam texts would complain. The likely actual number of texts sent, therefore, would be much higher than this.<br><br>The notice concluded that this was a serious and deliberate breach of the Privacy & Electronic Communications Regulations of a kind likely to cause substantial distress. Readers may remember that both the company and its sole director were prosecuted, in October, for failure to notify the company's data processing activities to the Information Commission. | **Monetary penalty of £175,000** |

# European data protection news

## Belgium

### Audit group to be set up by the Belgian Data Protection Commission

**Cédrine Morlière, *Senior Associate, Bird & Bird (Brussels)***

In the context of recent privacy breaches in Belgium, mainly related to the leakage of customer data by a Belgian public transport company and the hacking of Belgacom's servers, the President of the Belgian Data Protection Commission has announced on the 21 October 2013, that it will install a **dedicated group to carry out on-site audits and actively investigate violations of citizens' data protection rights**.

The group will be working in collaboration with the Computer Crime Unit, the Telecom Regulator and the Cyber Emergency Team.

# Czech Republic

## New Position of the Czech Data Protection Authority enlightening the records of phone calls

**Andrea Jarolimkova, *Associate,* Bird & Bird (Prague)**

In October 2013, the Czech Data Protection Authority ("**DPA**") issued its Position No. 5/2013 on Making Voice Records within the Electronic Communication in Relation with the Provision of Services from the Perspective of Data Protection Law. Its purpose is to cast light on cases when the phone calls with customers or clients, especially in frame of operations of various call centres, are recorded for different purposes not always fully compliant with legal requirements. The DPA therefore provides with more explanations describing their opinion to this topic.

In case of calls to customers' lines, a customer is most often informed at the beginning of a phone call that: "*This call can be monitored for quality assurance*." According to the DPA, there are only two legitimate purposes for which the voice records can be made. Firstly, the conclusion and the fulfilment of a contract between the data controller and its clients, and secondly, so called improving quality of services. If the personal data processing is essential for conclusion or, fulfilment of a contract with the client, the data controller can generally process personal data without the consent of the client and employees. In contrast, should personal data be processed for the purpose of improving quality of services, the client's informed consent is necessary. Most importantly, the DPA expressed its view that if the client continued in a call after receiving information about monitoring, it did not constitute the consent with the processing of personal data. According to the DPA, the "active" consent from customers has to be obtained prior to a recorded call, e.g. contained in an agreement in case of current customers, or via a separate option in a voice self-service in case of prospective or other customers. Also processing of employees' data for the purpose of improving quality services is, similarly to the fulfilment of legal obligation, possible without their consent, but it must not breach their privacy and personal life.

# France, Spain and the Netherlands

**French and Spanish Data Protection Authorities impose fines on Google**

In March 2012, Google merged into a single privacy policy its different rules applicable to sixty services, including Google Search, YouTube, Gmail, Picasa, Google Drive, Google Docs, Google Maps, etc. because of the number of services involved, almost all European Internet users were affected by this decision.

Both the French Data Protection Authority ("**CNIL**") and the Spanish Data Protection Agency ("**SDPA**") said that Google's privacy policy was not in compliance with national data protection regulations, regarding the following areas:

- Information provided to users
- The legitimate basis for the processing of personal data
- Consent to cookies
- Data retention periods

On 19 December 2013, the SDPA imposed a fine of **EUR 900,000** upon Google Inc., and on 3 January 2014 the CNIL followed suit and issued a fine of **EUR 150,000.** On 7 February 2014, the French Supreme Court ("Conseil d'Etat") rejected Google Inc.'s appeal against the CNIL's sanction. Following this, Google has announced that it will comply with the French Supreme Court decision and post a notice on its website relating to the decision.

**The Netherlands**

The Dutch DPA has also investigated Google's privacy policy and his holding a hearing with Google to discuss its preliminary conclusion.

# Hong Kong

## Leakage of Internal Documents by the Hong Kong Police Force

**Marcus Vass, *Partner,* and Frankie Tam, *Associate,* Bird & Bird (Hong Kong)**

The Privacy Commissioner for Personal Data (the "**Commissioner**") conducted an investigation against the Hong Kong Police Force ("**HKPF**") in relation to a data leakage of police documents containing personal data.

Background of the Incident
In September 2012, the media reported that police documents could be found on a peer-to-peer file sharing software called Foxy. The documents leaked include 210 copies of witness statements, HKPF's internal memoranda, forms and correspondence containing personal data such as names, Hong Kong Identity Card numbers, addresses and details of the prosecution of arrested persons.

The HKPF internal investigation revealed that a police officer (the "**Police Officer**") had occasionally used his private USB thumb drive to download documents to his own computer (the "**Computer**") and used the Computer for work purposes. The Police Officer eventually sold the Computer. Before selling the Computer, the Police Officer had tried to delete all the information in the hard disk by an erasure software. However, he did not remove the hard disk or use the software approved by the Chief Systems Manager. The leaked documents could have been recovered from the hard disk after sale of the Computer, and the data was subsequently leaked.

The Findings of the Commissioner
Data Protection Principle ("**DPP**") 4 under the Personal Data Privacy Ordinance (Cap. 486) ("**PDPO**") provides that a data user must take all practicable steps to ensure that personal data are protected against unauthorized or accidental access, processing or erasure. The HKPF is a data user and must comply with DPP4.
In examining whether the HKPF had contravened DPP4, the Privacy Commissioner considered two aspects:

(1) whether the HKPF had any policy in place to safeguard personal data; and
(2) whether the HKPF had taken adequate measures to ensure that its officers knew, understood and complied with the policy.

The Privacy Commissioner considered that if there was only policy in place but there was no mechanism or practical measures implementing the policy, the HKPF could still contravene DPP4.

The Commissioner noted that the HKPF has in place the Police General Orders ("**PGO**") and the Force Information Security Manual ("**FISM**"). The PGO and the FISM contain the following information security requirements (the "**Requirements**"):

- Security measures such as encryption using HKPF provided tools, and password protection of electronic files/data shall be taken to protect sensitive or classified information.

- HKPF members are not permitted to use their private ICT [information and communications technology] equipment (e.g. memory cards, USB thumb drives) to process or store electronic information unless written approval has been obtained from their Formation Commander.

- HKPF members shall not carry any electronic data of or above 'Confidential' classification off police premises unless prior approval has been obtained.

- Classified information must not be processed or stored in privately owned computers and privately owned portable electronic storage devices, such as USB storage devices, Flash memory cards, except with the written approval from the Formation commander of SP rank or above.

- User who wishes to withdraw privately owned computers for official use at work shall notify the Formation Information Technology Security Officer ("**FITSO**") seven days before removing it from the formation. The FITSO shall conduct a physical inspection of the hard disk drive and all data storage media containing official information to ensure that all data connected with official purposes are securely erased, by using an approved software.

- Before the removal for repair or the transfer of ownership of any privately owned computer which has been approved for duty purposes, the hard disk shall be physically removed or securely erased, by using approved software, of all data relating to the officer's official duties. The officer shall not allow unauthorized persons' access to the information on the hard disk.

The HKPF had used various means to inform police officers of the PGO and FISM, including sending email reminders to all officers and the provision of four relevant training sessions to the Police Officer.
In light of the Requirements in place and the practical measures adopted by the HKPF, the Commissioner is of the opinion that the HKPF has taken adequate steps to formulate appropriate policies, devise a system to safeguard data and implement enough measures under this system. The leakage incident was seen as an isolated incident of human error which does not constitute contravention of DPP4 on the part of the HKPF. The Commissioner commented that the obligations of data users are not absolute and they are not expected to prevent data leakages at all costs. This case shows that carelessness of an employee can undermine sound privacy policies of an organisation. In his concluding remarks, the Commissioner opined that the building of a culture of privacy is imperative to ensure an organisation-wide commitment.

**A Look Back at 2013 in Statistics**

The investigation report summarised above is one of the six reports published by the Commissioner's Office in 2013. The Commissioner's Office received 1,792 complaints in 2013. There was a 48% increase compared with 2012.

This record high number of complaints reflects more public awareness of data protection in Hong Kong.

Of the 1,792 complaints received, 78% were made against organisations in the private sector.

Almost 30% of the complaints received by the Commissioner's Officer were related to use of personal data in direct marketing. The number of complaints related to the use of new information and communications technologies ("**ICT**") has also increased substantially from 50 in 2012 to 93 in 2013.

As regards enforcement and prosecution, the Commissioner's Office issued 32 warnings and 25 enforcement notices in 2013, compared with 27 warnings and 11 enforcement notices in 2012. 20 cases were referred to the Police for consideration of prosecution. This is an increase of 33% compared to 2012. Among the 20 cases, 14 cases were related to contraventions of the direct marketing provisions.

The Commissioner' Office has indicated that their strategic focus for 2014 will be in the following areas:

a) increased use of mobile apps;

(b) the need for organisations to embrace corporate governance responsibilities relating to data protection and adopt holistic privacy management programmes; and

(c) regulatory issues concerning cross-border flows of personal data.

# Italy

## Data protection update on recent Garante decisions, authorities and guidance

**Debora Stella, *Associate*, Bird & Bird (Milan)**

### Authorisations for retention of CCTV imgages for a period of time that is longer than the maximum statutory retention period

a) The company XY, manufacturing magnetic cards and cards with contact or contactless microchips, mainly for credit card companies, filed a request of prior checking to install a CCTV system with a retention period of the images of 90 days instead of the statutory maximum period of 7 days. The Italian DPA authorised the 90 day retention period in the areas of the building where there is a high risk of offences, in consideration of the company's specific activities and the need of higher security procedures (dated October 24, 2013).

b) The company Società Generale d'Informatica S.p.a. (Sogei), controlled by the Ministry of Economy and Finances, filed a request of prior checking to install a CCTV system with a retention period of 30 days instead of the maximum statutory 7 days period. The company operates several strategic information and databases including "classified information". The Italian DPA authorised the 30 days retention period to the company, in consideration of its peculiar and delicate activities and the need of higher security procedures (dated 28 November 2013).

### Call centres

The Garante issued a general decision (dated 10 October 2013 doc. Web n. 2724806) to impose specific requirements to controllers who, autonomously or through service providers, use call centres.

Those requirements include:

a) Clear information about where the operator is located;

b) In case of inbound calls, procedure to let the user choose an operator situated in Italy; and

c) In case of transfer of personal data to another call centre located outside the EU to transmit a communication to the Garante (model form available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2722504).

### Department of Information and Security (Dis)

On 11 November 2013 the Garante signed an agreement with the Department of Information and Security (Dis) to guarantee security and transparency to personal data accessible to the Italian Intelligence.

In particular the agreement regulates the inspection that the Garante can put in place and the communication by the Intelligence to the Garante about what kind of data the Intelligence has access to.

### Remote mobile payment

The Garante launched at the beginning of January 2014 a public consultation regarding the Draft Guidelines on remote mobile payment (doc. Web n. 2830145); deadline for contributions is March 4, 2014.

Further to the implementation in Italy of the Directives 2007/64/EC (Payment Service Directive) and 2009/110/EC (e-Money Directive) the Garante intended to provide detailed guidance on how to comply with the data protection requirements. Once approved, the Guidelines will be mandatory for the operators to which they are addressed, i.e.:

a) the operators, as the providers of electronic communications network and services publicly available, providing payment services to their customers through their mobile phones (either by debt on their pre-paid card or by charging their bill);

b) the aggregators (Hub): as the entity who implement and manage the web application needed to make possible the transfer of products and digital services;

c) the merchant, as the entity which sell digital contents to the public.

In particular the Draft Guidelines provide detailed instructions on how and when to provide the privacy notice and collect the consent, where necessary. The Garante also identified peculiar and specific security measures that the operators/hub and merchant will have to implement as well as a retention period for data up to a maximum of 6 months.

# Poland

**Reduced requirements for data transfer outside the EU**

**Izabela Kowalczuk, *Associate,* Bird & Bird (Warsaw)**

The Polish government has proposed amendments to the Personal Data Protection Act of 29 August 1997 (the "**Bill**"). The changes concern two main issues:

a) transition of the functions of the data protection officer, known in Poland as the information security administrator. We reported on this issue last year. Please see the link here Draft amendment of the Personal Data Protection Act
b) facilitation of transfer of personal data to a third country that does not ensure an adequate level of protection.

It is envisaged that the Bill will be enacted by the beginning of 2015.

**EU Model Clauses**. Currently, a data controller who wants to export personal data to a third country not ensuring an adequate level of protection based the EU Model Clauses approved by the European Commission needs to obtain prior consent of the Inspector General for Protection of Personal Data ("**GIODO**"). Such approval takes up to six months in some cases. This also means that data controllers have to obtain a new GIODO consent each time the scope and purpose of the transfer change. Thus, the current regulation creates an administrative burden for organisations and is a far-reaching formality.

Under the Bill, GIODO's consent will no longer be required if a data exporter and a data importer enters into agreement based on the EU Model Clauses.

**BCRs.** So far, the Personal Data Protection Act has been silent about binding corporate rules ("**BCRs**") which are internal rules (such as a Code of Conduct, global policy) adopted by multinational group of companies with regard to international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. In practice GIODO approved BCRs. The Bill introduces explicit regulation giving GIODO's authority to approve BCRs as a basis for personal data transfers to other controllers or data processors within the same group in a third country.

The Bill also explicitly allows GIODO to conduct consultation with other EU data protection authorities, in particular BCRs. While issuing the decision GIODO takes the results of this consultation and approvals of BCRs by other data protection authorities into account, if any were issued.

The proposed changes are moving in the right direction – to facilitate the data transfer without lowering the level of personal data protection. This is a good signal for international companies which will not be obliged to obtain GIODO's consent each time they decide to launch a new product involving data transfer to a third country.

The Bill is available in Polish here:

http://legislacja.rcl.gov.pl/docs//2/181358/181362/181363/dokument87482.pdf

# Switzerland

***Sylvain Métille, Head of Technology and Privacy, and Ariel Ben Hattar, Junior Associate,***

***BCCC Attorneys-at-Law LLC (Lausanne)***

## 1. Guidance on the use of cloud computing in a school environment

On 31 Ocotober 2013, Privatim, the association of the Swiss data protection commissioners published a leaflet on its website on the use of cloud computing in a school environment. The leaflet draws the schools' attention on the data protection-related regulation that applies to the use of cloud computing. In this regard, Privatim reminds the schools that it is their duty to ensure a lawful treatment of the relevant data.

Several conditions shall be met, among which a written agreement between the school and the provider of the cloud computing services. It should be noted, however, that the terms and conditions of the contract cannot be modified unilaterally for the agreement to comply with data protection regulations. In addition, the place where the data collected by the cloud computing service provider is processed must be known to the school and any change must be approved. Furthermore, additional conditions must be met when data is transmitted abroad.

The leaflet concludes that it seems doubtful that schools can indeed use the services of the likes of Google Drive, Dropbox and Microsoft Office 365, considering the services providers use general business conditions and retain the right to modify it at any time, at best upon prior notice, have their datacenters outside of Switzerland and use contracts that almost never provide a place of jurisdiction in Switzerland.

http://www.privatim.ch/fr/privatim-publications/cloud-computing-aux-ecoles.html (available in French, German and Italian)

## 2. Impact assessment tool

On 26September 2013, the Federal Data Protection and Information Commissioner ("**FDPIC**") published a tool on its website aimed at helping companies and administrative bodies assess the impact of their new projects in terms of data protection. The tool takes the form of a questionnaire where the company or administrative body is asked about the details of its new project in terms of data protection: i)what kind of data will be used during the project; ii)will the persons whose data are collected be informed and have a right to access their data; and iii) is it forecasted to transfer some of the data collected abroad; etc. At the end of the questionnaire a score card is displayed, listing the main issues surrounding the project by theme (transparency, security, lawfulness, etc.).

http://www.edoeb.admin.ch/datenschutz/00626/00743/01128/index.html?lang=fr (available in French, German and Italian)

## 3. FDPIC "note" on the transmission of personal data to U.S. authorities by Swiss banks

On 20 June 2013, the FDPIC published a note drawing the Swiss banks' attention on the fact that the transmission of personal data, including in the context of the fiscal dispute between the U.S. and Switzerland, is

subject to the Data Protection Act. This note follows the October 15th, 2012 recommendation by the FDPIC.

In its June 2013 note, the FDPIC reminds, among others the banks that the following key principles apply:

- -Transparency: the bank must inform the persons *before* transmitting their personal data. This also applies to non-natural persons;
- -Justification: in case a person refuses that its data be transmitted, the bank must weigh the competing interests and provide proper grounds for the transfer of data;
- -Legal proceedings: if a bank decides to transmit data against the will of the person whose data is transmitted, said person may take legal action against the bank.

Furthermore, the FDPIC summoned the banks to inform it of their forecasted data transmissions.

http://www.edoeb.admin.ch/aktuell/index.html?lang=fr (available in French, German and Italian)

## 4. FINMA Circular on operational risks - banks

On 29August 2013, the Swiss Financial Market Supervisory Authority FINMA ("**FINMA**") published an amended version of its 2008 circular on operational risks in the banking sector to take the new so-called Basel III recommendations into account. While the circular mainly focuses on risk tolerance and capital requirements, it also contains new provisions on how banks should handle customer data. Among the requirements set forth by the amended circular, banks should classify their clients' data by taking into account the way said data identify, or could identify if matched, the clients. Furthermore, access to clients' data must be granted on a "need to know" basis.
The amended data protection-related provisions of the circular will enter into force on 1 January 2015.

The amended circular follows a number of high profile clients' data leaks within banks over the past years that recently lead the FINMA to issue a formal reprimand against one of the banks that was subject to the leaks, as the FINMA considered that the bank was not organised appropriately in order to avoid the leak that occurred.

http://www.finma.ch/f/aktuell/Pages/mm-rs-opr-risiken-banken-20130110.aspx (available in French, German and Italian)

# twobirds.com

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