Bird & Bird

International data protection enforcement bulletin – October 2013

Welcome to the October 2013 International data protection enforcement bulletin.

In addition to a review of enforcement action taken in many of the jurisdictions in which Bird & Bird has offices, highlights this quarter include:

- The privacy implications of the use of Drones across the EU
- An update on subject access requests in the UK, following new guidance from the data protection authority
- The impact of an IT security Recommendation being introduced Poland, affecting the banking sector
- A round-up of data protection principles affected by recent decisions by the Italian DPA

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

Ruth Boardman

Partner

ruth.boardman@twobirds.com

Laura Acreman

Associate

laura.acreman@twobirds.com

Enforcement tables by country

Czech Republic

Date	Infringing entity	Details of infringement	Sanction(s) imposed
May 2013	Czech Republic Prison Service	Following the unlawful release of photographs of a high-profile politician in custody to the press, it was found that all Prison Service employees had equal access to the prison information system, so employees from other prisons could also access personal data of imprisoned persons. Furthermore, access rights did not prevent the unauthorised reading, copying or transferring of records containing personal data of imprisoned persons.	**CZK 50,000 fine** (approximately EUR 2,000)
May 2013	MAFRA a.s.	The operator of news website "iDNES.cz" did not remove a comment from the discussion under an article, despite the fact that the Police requested information about the author of the comment for criminal proceedings. The comment contained information revealing the identity of a juvenile rape victim.	**CZK 35,000 fine** (approximately EUR 1,400)
June 2013	ZnamyLekarz Sp.z.o.o.	Personal data of Czech health care workers were published without their consent on the website of the Polish company "www.znamylekar.cz". Users of the website could appraise the health care workers in a discussion forum.	**Measures for remedy**

France

Date	Infringing entity	Details of infringement	Sanction(s) imposed
11 April 2013	Total Raffinage Marketing	In August 2012, the CNIL received a complaint from a trade union of Total Raffinage Marketing regarding the organisation of professional elections by electronic means. Following this, the CNIL carried out an inspection of the election system. Several defaults concerning security and confidentiality of data were identified during the inspection: • The election was organised without a prior test of the vote's system in order to ensure that the system was working properly; • Identifiers and passwords for voting were not being sent to employees in a secure way; • The electronic ballot was not encrypted. The CNIL considered that Total Raffinage Marketing failed to comply with its obligations on security of data under article 34 of the French DP Act.	The CNIL issued a **public warning** to Total Raffinage Marketing.
30 May 2013	PS Consulting (SAS Professional Service Consulting)	In December 2010, the CNIL received a complaint from an employee of PS Consulting concerning CCTV usage. During the first inspection, the CNIL identified several breaches: the CCTV cameras were permanently monitoring employees' activities, employees were not adequately informed about the system and the security measures for accessing images were insufficient. The CNIL therefore asked PS Consulting to remedy these breaches and PS Consulting made commitments to do so. However, during the second inspection in October 2012, the CNIL established that the CCTV system had not been modified and that PS Consulting was still failing to comply with its requirements under French DP law.	PS Consulting was **fined EUR 10 000** by the CNIL.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
19 June 2013	BNP Paribas	In 2008 and 2009, the CNIL received several complaints from BNP PARIBAS' customers concerning the persistence of their registration in the National Register of Household Credit Repayment Incidents (*FICP*) maintained by the Bank of France (*Banque de France*) despite payment of their debt, sometimes for several years. In February 2010, the CNIL asked BNP to comply with its obligation to update customer data in the FICP within four days upon the customers' payment as required under applicable legislation, by notifying it to the Banque de France in order to delete the name of the customer from the Register. However, between 2011 and 2012, the CNIL received new complaints based on the same grounds. The CNIL concluded that BNP Paribas failed to comply with its obligation to update its customers' data under article 6-4° of the French DP Act.	The CNIL issued a **public warning** to BNP Paribas.
25 June 2013	Bout-Chard	An action was brought against the Bout-Chard company to nullify the sale of a client database, for the reason that the database had not been registered with the CNIL. The Court of Appeal in Rennes rejected the claim for the sale to be nullified. They found that Bout-Chard's customer database ought to have been registered with the CNIL but considered that French law does not provide that the absence of such a notification should be sanctioned by nullification. However, the French Supreme Court (*Cour de Cassation*) overruled the decision of the Court of Appeal and concluded that the sale of a client database was null and void on the account of having an unlawful object, as it had not been registered with the CNIL.	The French Supreme Court **nullified the sale of the client database** for the reason that the database had not been registered with the CNIL.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
12 July 2013	E.Leclerc	Following a complaint regarding the use of CCTV in an E.Leclerc mall in Bourg-en-Bresse, the CNIL conducted an on-site inspection which revealed the existence of a disproportionate system which was placing employees under constant scrutiny and was notably used to monitor working hours of employees. The CNIL inspection also established that individuals being filmed were not appropriately informed, the retention period for the images was too long and there was a lack of adequate security of data collected under the system.	The CNIL decided to make public the **formal notice** to E.Leclerc, requiring a revision of its CCTV system within a period of 3 months.
29 August 2013	Paris Saint-Germain Football (PSG)	Following several complaints and articles in the press regarding the existence of a black-list of PSG's supporters, the CNIL decided to carry out an on-site inspection in the premises of the football club. The on-site inspection revealed the existence of two black-lists: one concerning persons subject to a stadium ban issued by relevant public authorities and another concerning "unwanted persons" that PSG considered as having a non-compliant behaviour with the values of the football club during football or handball matches. None of the lists could be legally maintained since their implementation was not first authorised by the CNIL as required in such a case under French legislation. The CNIL also established that these lists were communicated to Paris Handball.	The CNIL decided to make public the **formal notice** to CNIL requiring the football club within a period of 1 month to : • File authorisation requests to the CNIL concerning the processing of data on persons subject to a stadium ban issued by relevant public authorities and on persons that the PSG considers as having a non-compliant behaviour with the values of the football club during matches; • To stop communicating the concerned lists to Paris Handball.

Hungary

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
May 2013	A health service provider	Following the removal of a wisdom tooth, the data subject requested the health service provider to provide the documentation relating to the operation (including X-ray picture, patient information etc.). This was rejected by the health service provider based on the grounds that the data subject can have access to the documentation via a different procedure. The National Authority for Data Protection and Freedom of Information (the "**Authority**") established that the data controller should have provided the documentation to the data subject through the provisions of the Hungarian Health Services Act. By failing to do so, the data controller infringed the relevant provisions of the Privacy Act and the Health Services Act.	The Authority imposed a **fine of HUF 300,000** (approx. EUR 1,000) **and** ordered the infringing entity to disclose the relevant health documentation.
May 2013	Asset Manager of Óbuda LLC (Óbudai Vagyonkezelő Zrt.) Mayor Office of the Municipality of Óbuda-Békásmegyer (Óbuda-Békásmegyer Önkormányzat Polgármesteri Hivatala)	The Asset Manager of Óbuda LLC requested personal data from citizens living in Óbuda (a district in Budapest), in order to review the rental value of the flats owned by the municipality. Social and financial data were requested on a special sheet. In addition to tenants' personal data, personal data of family members or others living in the given apartment were requested. The Authority established that although the Mayor Office of the Municipality of Óbuda-Békásmegyer qualifies as the data controller on the basis of a municipality decree, the Asset Manager of Óbuda LLC acted as the data controller without having any legal basis to do so. The Authority also established the consent incorporated into the special sheet does not meet the requirement of voluntary consent, and neither does it provide adequate information.	The Authority imposed a fine of: • **HUF 400,000** (approx. EUR 1,300) on the Asset Manager of Óbuda LLC; and • **HUF 500,000** (approx. EUR 1,670) on the Mayor Office of the Municipality of Óbuda-Békásmegyer.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
May 2013	Generál Média Publishing Kft.	The infringing entity operates approximately 40 websites and was the data controller of 20 websites, offering different types of services. In case of dating websites the Authority established that the data controller did not apply age restriction measures during the registration process, so children under the age of 16 could register without requiring the approval /consent of their parent or guardian. 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. Furthermore, although the data controller stated that data subjects could unsubscribe from newsletters, in practice this was not true and data subjects received newsletters on a weekly basis even after unsubscribing. The 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 3,000,000** (approx. EUR 10,000) **and** ordered the infringing entity to: • delete the unlawfully processed data or obtain the consent of the data subjects' guardians for the registration; • modify the existing practice relating to obtaining consent to send out newsletters in order to comply with privacy provisions; and • allow data subjects to unsubscribe from newsletters.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
May 2013	Analysis Hungarien Group Kft. Gapelaag Kft.	The company Analysis Hungarien Group Kft. organised product presentations under the name of "Health Day" and invited people through the phone book. To those people who become interested the company sent an invitation to the product presentation event. At the event, a consent form was handed over to data subjects. If individuals intended to buy the products presented at the event, they entered into a product sale agreement with Gapelaag Kft. The Authority established that both companies qualify as data controllers because they determine the purpose and scope of the data processing. The Authority furthermore established that the consent form does not meet the requirement of providing detailed information to data subjects about the purpose of data processing, the data controller and the rights of the data subjects. Moreover, the consent form does not meet the purpose-bound data processing requirement and the principle of necessity. In addition, during the event the organisers recorded the ID numbers and social security numbers of visitors, which is not permitted under relevant laws.	The Authority imposed a fine of: • **HUF 2,500,000** (approx. EUR 8,300) on Analysis Hungarien Group Kft.; and • **HUF 200,000** (approx. EUR 670) on Gapelaag Kft.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
June 2013	EOS Faktor Zrt.	The infringing entity used the personal data of individuals who did not qualify as debtors for collecting debts (factoring). The infringing entity did not enter into any form of agreement and the data subjects received violent and aggressive calls and SMS messages from the infringing entity. When the data subjects requested the deletion of their personal data (i.e. phone number) additional personal data (i.e. name) was requested or the request was rejected. The individuals concerned (especially neighbours and relatives) were contacted by the infringing entity in case the debtors could not be reached, in order to force the debtor to pay. The individuals concerned were called by using the phone book and the call logs were recorded in an electronic register. The Authority contacted the Hungarian Supervisory Authority ("HSA") and received information that the HSA prohibited the infringing authority's unfair market behaviour and imposed a consumer protection fine upon them. The Authority established that during the phone calls the data controller did not obtain consent from the individuals not qualifying as debtors for the processing of their voice recordings, name, address and phone number. Furthermore, no information was provided to the data subject during the phone calls.	The Authority imposed a **fine of HUF 6,000,000** (approx. EUR 20,000) **and** prohibited unlawful data processing by ordering the deletion of personal data of individuals not qualifying as debtors.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
June 2013	RSG Direct Kft. Datahouse Central Europe Kft. Sanoma Media Budapest Zrt.	RSG Direct Kft. and Datahouse Central Europe Kft. organised a prize contest. The aim of the contest was to create a database on the basis of which advertisements can be sent both via post and electronic methods. The prize contest appeared on the website operated by Sanoma Media Budapest Zrt. with the original intention being to perform the collection of personal data by using a so-called double opt-in system and the check box solution where the data subject gives his/her personal data on a web surface, then receives a confirmation e-mail containing his/her personal data. The system would have only considered the data subject's consent to data processing and receiving direct marketing materials given if the data subject clicked on the link provided in the confirmation e-mail. Contrary to the above, the system was set up differently and it did not collect e-mail addresses and it did not sent out confirmation e-mails. Although data were collected, these data were not used at all. The Authority established that the requirement of providing adequate information was not met because there was no information on the website of the prize contest about any relevant privacy policy and terms and conditions. Furthermore, the language of the terms and conditions was not clear and was difficult to follow. The data subjects were not informed about the purpose of data processing. In addition the Authority established that the infringing entities did not make necessary steps to obtain the data subjects' unambiguous and express consent. It was also established that no option was available for data subjects to revoke their consent.	The Authority imposed a fine of: • **HUF 300,000** (approx. EUR 1,000) on RSG Direct Kft.; • **HUF 100,000** (approx. EUR 340) on Datahouse Central Europe Kft.; and • **HUF 600,000** (approx. EUR 2,000) on Sanoma Media Budapest Zrt..

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
July 2013	Unknown	The infringing entity is one of the leading real estate brokers in Hungary operating a website and arranging property visits. During these property visits, participants were asked to sign a special document ("statement of visiting"), however, they were not informed of the legal basis and the purpose of the data recording. Based on the above the Authority established that requirement of providing detailed and adequate information to data subjects and the principle of necessity and lawful purpose were not met, therefore the data processing was unlawful.	The Authority imposed a **fine of HUF 700,000** (approx. EUR 2,340).
August 2013	Unknown	The infringing entity sent pre-application forms and cooperation statement documents to its members for the purpose of organising language courses. In these documents, personal data such as name, address, place and date of birth, phone number social security number and trade union membership details were requested. Providing these data was mandatory. In addition, copies of ID cards and social security cards were requested. Information on the language courses was sent in one e-mail to more than 800 recipients. As a result the e-mail addresses of the data subjects were disclosed to others. The Authority established that the provisions of the Privacy Act were infringed because personal data (i.e. e-mail address) were transferred without the consent of the data subjects and the infringing entity did not ensure the adequate protection of personal data.	The Authority imposed a **fine of HUF 100,000** (approx. EUR 340).

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

Italy

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
18 October 2012 (Recently published)	Fastweb S.p.A.	The decision followed complex legal proceedings connected with previous proceedings against the same company (one of the major telecommunication operators in Italy) and other data controllers (see case law below). In the decision dated June 26, 2008, the Italian Data Protection Authority prohibited the company from processing of data for telemarketing purposes, from a database of phone contacts created before 01 August 2005. According to the Authority, the company was not entitled to legitimately use the database without the prior consent of the contacts. The company did not adhere to the decision imposed and acquired a database of personal data from another company (Edipro s.a.s.), creating a fictitious data controller-data processor connection. As a result, the company obtained the database and used the contacts for marketing purposes, without giving clear information and without obtaining valid consent. It was also found that that the company made several unsolicited promotional telephone calls.	**The Italian Data Protection Authority:** Fined the company with a total amount of **EUR 300,000**, by way of a pecuniary administrative sanction for offences referred to in article 164-*bis*, paragraph 2 of the Italian DP Code (i.e. several offences committed in relation to a database of a significant size).

[1] This table contains the most important cases that were examined and published by the Garante in recent months. Claims made against banks and credit information companies regarding the exercise of data subject rights have not been included.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
10 January 2013	Consodata S.p.A	Following a previous decision dated 26 June 2008, the Italian Authority prohibited the company (one of the major Italian provider of databases for marketing activities) from processing personal data contained in a telephone directory published before 01 August 2005 for telemarketing purposes, without providing valid information and obtaining consent. The company did not observe the provisions of the aforementioned decision; and continued to use and sell the database to several of its customers without valid consent. In addition, the company processed personal data contained in a lifestyle database for profiling and targeting purposes and transferred it to several of its customers without obtaining separate consent for each of these purposes. Further data processing was found to be in violation of the data protection law, as the company was processing and transferring personal data extracted from poll lists for marketing purposes. The processing of this information for marketing purposes is prohibited by art. 177, par. 5 of the Italian DP Code. Finally, the company unlawfully processed for marketing purposes also personal data contained in an additional database of e-mail contacts obtained from its business partners failing to collect the contacts' consent to its own marketing activities.	**The Italian Data Protection Authority:** Fined the company with a total amount of **EUR 400,000**, by way of a pecuniary administrative sanction for offences referred to articles 162, paragraph 2-*bis* and 2-*ter* (i.e. the unlawful processing of personal data) and 164-*bis*, paragraph 2 of the Italian DP Code (i.e. several offences committed in relation to a database of a significant size)
07 February 2013	Edipro S.a.s.	The company transferred all personal data from its database "DB consumers Italia" to Fastweb S.p.a. for Fastweb telemarketing purposes, without the prior, free and specific consent of the data subjects. Furthermore, the seriousness of the matter resulted from the fact that the unlawful transfer of personal data has been established on the basis of a fictitious data controller-data processor relationship; and following this transfer, unsolicited calls had been made to millions of users.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 100,000**, by way of a pecuniary administrative sanction for the offences referred to in articles 162, paragraph 2-*bis* (i.e. the unlawful processing of personal data) and 164-*bis*, paragraph 2 of the Italian DP Code (i.e. several offences committed in relation to a database of a significant size)

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
31 January 2013	Edizioni associate S.r.l.	This case concerned the alleged unsolicited promotional emails sent by the company. It was found that the company proceeded to unlawfully process data of users listed in a database purchased from a third party without giving notice to, and obtaining the consent of, the data subjects.	**The Italian Data Protection Authority:** Fined the Edizioni associate S.r.l. with an amount of **EUR 16,000**, by way of a pecuniary administrative sanction for offences referred to in articles 161 and 162, paragraph 2-*bis* of the Italian DP Code.
31 January 2013	Smart s.n.c.	This case concerned a single unsolicited commercial fax sent from the company without the data subject's prior consent.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 8,000**, by way of a pecuniary administrative sanction for offences referred to in article 162, paragraph 2-*bis* of the Italian DP Code.
January 31, 2013	Banca Popolare dell'Etruria e del Lazio	The claimant requested the bank for an intelligible copy of his personal data relating to all buying and selling stock activity made through its bank accounts, under articles 7 and 8 of the Italian DP Code. The bank stated that such requests for access was to be rejected unless payment of the relevant fees have been made, since the request did not qualify as an exercise of data protection rights (which are free of charge), but as a request connected to the bank's contractual relationship (subject to charges).	**The Italian Data Protection Authority:** Confirmed that the matter is governed by data protection rules, and ordered the bank to provide a copy of the documents requested within 45 days.
January 31, 2013	Banca Popolare del Mezzogiorno S.p.A	The claimant requested the bank for an intelligible copy of his personal data relating to the statements of his account from the last five years, from the end of the financial relationship or from the last registration. The bank stated that such requests for access was to be rejected unless payment of the relevant fees have been made, since the request did not qualify as an exercise of data protection rights (which are free of charge), but as a request connected to the bank's contractual relationship (subject to charges).	**The Italian Data Protection Authority:** • Confirmed that the matter is governed by data protection rules and ordered the bank to provide a copy of the documents requested within 60 days. • In addition the bank was ordered to pay **EUR 400** to refund the fees for the claim.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
07 February 2013	Primi sui Motori S.p.a.	The company sent out several unsolicited marketing emails to a business entity. The data was purchased from a third party but the company neither provided notice nor checked whether the business entity ever gave consent to this processing.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 23,000**, by way of a pecuniary administrative sanction for offences referred to in articles 161 and 162, paragraph 2-*bis* of the Italian DP Code.
07 March 2013	Aruba S.p.A.	The company did not obtain consent for unsolicited marketing communications to users who registered to the site. It argued that the processing felt under the exemption provided by the Italian DP Code (soft opt-out).	**The Italian Data Protection Authority:** • Confirmed that the exemption was not applicable since the products offered through the marketing e-mails were different from those the users expected when registering on the website. • Prohibited any further processing of the information.
04 April 2013	Discotape di Filippin Angelo & C. snc	The company unlawfully processed personal data by fraudulently activating phone cards in the name of unaware data subjects without providing an adequate information notice.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 12,000**, by way of a pecuniary administrative sanction for the offences referred to in article 161 of the Italian DP Code.
04 April 2013	Società editrice siciliana s.p.a	The company installed 19 security cameras in its building (some of which concealed inside smoke detectors) for property safety purposes, without providing adequate information to its employees and in violation of employment legislation requiring the prior agreement of the trade unions. Furthermore, the company processed personal data of the subscribers of its newspaper "Gazzetta del Sud" for marketing purposes without giving adequate information.	**The Italian Data Protection Authority:** • Declared the CCTV data processing unlawful, prohibiting any further use of the images. • Ordered the company to give a complete information notice to the subscribers.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
04 April 2013	Comune di Lascari	The municipality of Lascari (PA) published on its official site, some municipal ordinances regarding mandatory commitment to sanitary treatments related to persons with mental and/or physical disabilities, containing sensitive data through the disclosure of health information.	**The Italian Data Protection Authority:** • Prohibited the municipality of Lascari from disseminating and publishing sensitive data via the internet. • Ordered the municipality to take measures to comply with the guidelines of the Italian DPA on processing data online by governmental bodies. • Ordered the municipality to take any necessary steps to have the major search engines (e.g. Google) remove the copy of the documents from the internet.
04 April 2013	Umana S.p.a.	The company, an employment agency, took copies of candidate's ID documentation during the first interview round for the purposes of verification.	**The Italian Data Protection Authority:** • Stated that the processing of personal data through acquiring and retaining copies of ID documentation for job interviews violates the principle of relevance in relation to the purposes for which they are collected or subsequently processed. • Prohibited any retention of copies of ID documentation of the job applicants.
11 April 2013	PLD S.r.l.	The company unlawfully processed personal data by fraudulently activating a huge number of phone cards in the name of several unsuspecting data subjects without providing an adequate information notice.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 100,000 (i.e. EUR 10,000 for each data subject**), by way of a pecuniary administrative sanction for the offences referred to in article 161 of the Italian DP Code.
11 April 2013	Diners Club Italia S.r.l.	The company in question did not appoint designated staff as persons in charge of the data processing (*incaricati del trattamento*) nor did it update the mandatory Security Document.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 40,000**, by way of a pecuniary administrative sanction for the offences referred to in article 162 paragraph 2-*bis* of the Italian DP Code.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
11 April 2013	Casa di cura La Quiete S.r.l.	The company failed to comply with its obligation to notify the Italian DPA in relation to clinical laboratory tests.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 40,000,** by way of a pecuniary administrative sanction for the offences referred to in article 163 of the Italian DP Code.
18 April 2013	Azienda Usl 5 di Pisa	The hospital installed a series of video cameras in order to protect the property, which were also to record the employees and patients. The cameras were installed without the conclusion of an agreement with the trade unions, which was in violation of art. 4 law n. 300/1970 The hospital also assigned the surveillance to a third party entity without appointing it as data processor.	**The Italian Data Protection Authority:** • Declared the processing of video camera data unlawful and unusable according article 11, paragraph 2 of the Italian DP Code. • Ordered the company to complete the procedures provided by art 4 l. n. 300/1970. • Ordered the company to produce a complete information notice according to art. 13 of the Italian DP Code. • Ordered the company to appoint the entity responsible for the surveillance as the data processor. • Ordered the company to adopt all necessary precautions in order to guarantee a high level of security.
24 April 2013	Comune di Bologna	The municipality of Bologna arranged a series of permits for parking and access to limited traffic zones, which were to be displayed on the vehicle. The permits displayed the name and surname of the holder.	**The Italian Data Protection Authority:** • Considered the provision of these permits as unlawful as it was in violation of articles 19 par. 3 and 74 par. 1 and 2 of the Italian DP Code. • Ordered the municipality to remove the names and surnames from the permits.
08 May 2013	Profile 2100 S.r.l. in liquidazione	The company sent out commercial communication by fax, without having provided previous information notice; and with no evidence of the obtaining consent from the recipient.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 10,400**, by way of a pecuniary administrative sanction for offences referred to in articles 161 and 162, paragraph 2-*bis* of the Italian DP Code.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
08 May 2013	I Pargoli S.n.c.	The nursery school had installed webcams inside its building which allowed parents to check on their children while they were at school. This circumstance is related to recent media reports on serious cases of child abuse over the years.	**The Italian Data Protection Authority:** • Declared the use of CCTV systems connected to the web disproportionate and unnecessary. • Prohibited the company from the further processing of the images already acquired.
22 May 2013	ASL Torino 3	The hospital did not acquire the consent (which was required in writing by the law) from patients in relation to some analyses carried out in the laboratory and in the emergency department.	**The Italian Data Protection Authority:** Fined the hospital with an amount of **EUR 10,000**, by way of a pecuniary administrative sanction for the offences referred to in article 162, paragraph 2-*bis* of the Italian DP Code.
30 May 2013	Liceo Scientifico Statale "Plinio Seniore" di Roma	A high-school installed video cameras in different areas of its building. The installation was made without the conclusion of an agreement with the trade unions and an appropriate notice was not provided. Furthermore, the school arranged for a system of biometrical data collection of employee fingerprints without complying with the obligation to promptly notify the DPA under article 37 of the Code.	**The Italian Data Protection Authority:** Declared the processing of CCTV data as unlawful and prohibited any further use of biometric data, while they reserved judgement on the failure to notify the DPA and the omission of the notice.
06 June 2013	Zoomarine Italia S.p.a.	The company acquired the full name and e-mail address of the subscribers of its webpage: www.zoomarine.it, without providing adequate notice. Furthermore, the company installed two video cameras at the entrance of its building without the required information notice.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 12,000**, by way of a pecuniary administrative sanction for the offences referred to in article 161 of the Italian DP Code.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
06 June 2013	7° Circolo Didattico "Egidio Giusti" di Taranto	The educational institute published a list of teaching staff who passed a competition, on its webpage. The list included the teacher's names along with their private address, mobile phone number and tax code number.	**The Italian Data Protection Authority:** • Prohibited the institute from further publishing the personal data. • Prescribed the institute to adopt the necessary and appropriate measures; and adapt future publishing on the webpage to be subject to provisions of the Italian DP Code.
13 June 2013	Mafeco S.r.l.	The company failed to include an information notice on the website.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 6,000**, by way of a pecuniary administrative sanction for offences referred to in article 161 of the Italian DP Code.
13 June 2013	BBJ S.r.l.	The company purchased a database from another company and transferred it to a third company for marketing purposes without providing any notice or obtaining consent of the data subjects.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 64,400**, by way of a pecuniary administrative sanction for offences referred to in articles 161, 162, paragraph 2-*bis* and 164-*bis*, paragraph 3 of the Italian DP Code.
27 June 2013	E-Business Consulting S.r.l.	The company received a complaint on an unsolicited commercial e-mail. It was found that the company did not provide any adequate notice and it did not obtain the consent of the data subject. In addition the company made untruthful declarations to the Italian DPA.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 16,400**, by way of a pecuniary administrative sanction for offences referred to in articles 161 and 162, paragraph 2-*bis* of the Italian DP Code.
27 June 2013	Rey2mond S.n.c.	The company failed to include an information notice on the website.	**The Italian Data Protection Authority:** Fined the company with an amount of **EUR 4,800**, by way of a pecuniary administrative sanction for offences referred to in articles 161 of the Italian DP Code.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
July 18 2013	Roberto Abate s.p.a. (A&O)	A supermarket installed video cameras in its store which were able to record imagines of the cash desks. Images were retained for 72 hours. The cameras were also installed without the conclusion of an agreement with the trade unions.	**The Italian Data Protection Authority:** • Declared the processing of the video camera data as unlawful. • Ordered the company to complete the procedures provided by art 4 l. n. 300/1970 (agreement with the trade unions). • Ordered the company to revise the retention period of the images to the actual necessities of the processing as is prescribed in the Video Surveillance Decision dated 08 April 2010 by the same Authority (i.e. 24 hours except in peculiar circumstances).
18 July 2013	Okcom S.p.A	The company, a provider of electronic communications services, was fined EUR 40, 000 in October 23, 2012 for not adopted measures of "strong authentication" as prescribed by the DPA's General Decision "Security In Telephone And Internet Traffic Data - 17 January 2008". The company continued to utilise a biometric recognition procedure.	**The Italian Data Protection Authority:** 1) Declared the processing of such biometric data as unlawful under articles 11 and 132 of the Code. 2) Ordered the company to implement specific computerised authentication systems that must be based on strong authentication techniques as prescribed in the General Decision of 17 January 2008.
18 July 2013	Ministero della giustizia - Dipartimento dell'amministrazione penitenziaria	The offices of the penitentiary police posted a list of officers for whom overtime was recorded for remuneration. The list was published every month and indicated the exact number of hours worked as well as the name and surname of the officers. In article 10, par. 9 of the "Accordo nazionale quadro per il personale appartenente al Corpo di polizia penitenziaria" 14 June 2007, it was provided that the officer has to be indicated in an anonymous way.	**The Italian Data Protection Authority:** • Declared the data processing as unlawful under articles 11 and 19 of the Code. • Prohibited the Ministry of Justice offices from further processing the personal data in the way described.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
01 August 2013	Liceo Scientifico Statale "Giuseppe Battaglini" di Taranto	The high school installed a system of biometrical data collection, namely fingerprints, in order to register the working hours of the teachers and employees.	**The Italian Data Protection Authority:** • Prohibited the school from further usage of the biometrical data collection system. • Considered the use of biometrical data for the simple registration of the working hours of the teachers to be unlawful regarding the principles of necessity, relevance and proportionality (article 11 par. 1 lett d) of the Italian DP Code).

The Netherlands

Date	Infringing entity	Details of infringement	Sanction(s) imposed
25 July 2013	Arnhem, Nijmegen and Urecht Universities of Applied Sciences ("hoge scholen")	DPA demands that these universities of applied sciences implement appropriate technical and organisational security measures.	None so far.
30 July 2013	Misc. Dutch municipalities	Fingerprints taken for biometric passports were collected and stored in a de-centralised database. After a nationwide public debate about the privacy implications of this database, the Minister of Interior decided to stop collecting and storing the fingerprints. The DPA now demands that municipalities remove any fingerprints already collected.	None so far.
22 August 2013	TP Vision Netherlands BV (producer of Philips Smart TV's)	TP Vision collects personal data through Philips Smart TV's. According to the Dutch DPA this is not done in a sufficiently transparent manner: data subjects may not know about the data collected and/or that the collection is optional. Furthermore, to the extent that cookie-rules apply, no consent has been asked for or provided. Finally, according to the DPA, TP Vision has not used processor agreements for the use of Google Analytics.	None so far.

Poland

Date	Infringing entity	Details of infringement	Sanction(s) imposed
18 April 2013 (II SA/Wa 812/13)	Association X	An individual requested GIODO to order Association X to stop processing their personal data on Association X's website in the context of the activity of his employer, arguing that Association X's actions are unlawful. GIODO rejected the request, indicating that the processing of the individual's personal data was performed in compliance with the Act, which states that the processing of personal data may take place without consent if it is necessary to pursue the legitimate purpose of the controller and this will not violate the rights and freedoms of the data subject . In this case the legitimate purpose was manifested in the scope of business of Association X, which was monitoring the professional activity of leasing companies including the individual's employer.	The individual filed a complaint against GIODO's decision to the Regional Administrative Court. The court upheld the decision repeating GIODO's argument. The individual filed a cassation appeal to the Supreme Administrative Court which set aside the contested judgment and referred the case back to the court of the first instance for reconsideration. The Supreme Administrative Court held that the processing of the individual's personal data was not required to describe the activity of his employer. The Regional Administrative Court held the judgement in accordance with the interpretation of the Supreme Administrative Court.
15 May 2013 (II SA/Wa 2063/12)	The Credit Information Bureau	An individual requested the Inspector General for the Protection of Personal Data ("GIODO") to order the Credit Information Bureau ("CIB") to remove the individual's personal data from a database. The individual argued that the cause for processing their personal data had already lapsed, making the CIB's actions unlawful. GIODO refused to issue the order, indicating that the Banking Law allows the CIB to process an individual's personal data.	The individual filed a complaint against GIODO's decision to the Regional Administrative Court. The Court upheld GIODO's decision stating that although the purpose for processing the data had lapsed it still exists without the means of enforcement. Furthermore, the Personal Data Protection Act ("Act") allows for the processing of personal data for a justified legal purpose, which in this case was deemed as the provisions of the Banking Law allowing the Bank to assess the creditworthiness of a client.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
16 May 2013 (II SA/Wa 911/12)	Company X	An individual requested GIODO to order Company X to cease processing their personal data, arguing that the reason behind the processing the personal data did not exist. GIODO denied the request, indicating that Company X acted in compliance with the Act by processing the individual's personal data for the purpose of pursuing claims against them.	The individual filed a complaint against GIODO's decision to the Regional Administrative Court. The Court upheld GIODO's decision using the same reasoning. In addition, the Court held that the issue as to whether the claim exists should be decided by the common court, not the administrative authority.
22 May 2013 (II SA/Wa 416/13)	Bank	An individual sued a bank with whom they had applied for a loan. The individual claimed compensation for the damage incurred as a result of making his personal data available to the National Banking Association for the purpose of assessing his creditworthiness. The court denied the individual's claim. The individual appealed and the Appellate Court also denied the claim. The individual filed a complaint with GIODO claiming that the processing of his personal data by the bank was unlawful. GIODO dismissed the complaint.	The individual filed a complaint against GIODO's decision to the Regional Administrative Court. The Court held that, pursuant to the Banking Law, banks are allowed to make the data of their clients available to other banks and associations of banks to the extent that it was necessary for performing banking activity; therefore it found the claim to be unfounded.
23 May 2013 (II SA/Wa 625/13)	Company B	An individual requested GIODO to carry out an audit on Company B to examine if processing the clients' data was lawful. The individual claimed that his personal data were obtained by Company B in violation of the law; therefore the processing of his personal data was unlawful. GIODO rejected the request, indicating that Company B was unaware that the data were obtained in violation of the law at the time it concluded the contract with the individual. After the court found the contract null and void, Company B processed the client's personal data for bookkeeping and tax purposes, which was a legal obligation for Company B.	The individual filed a complaint against GIODO's decision to the Regional Administrative Court. The court upheld the decision repeating GIODO's argument. In addition, the court stressed that a personal data administrator has a special legal obligation to determine if the data were obtained lawfully. However, this was not the case here because Company B was unaware that the data were obtained in violation of the law.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
17 June 2013 (II SA/Wa 152/13)	Company C	An individual requested GIODO to order Company C to reveal the IP address of the user of a web portal administered by Company C. The individual claimed that the user infringed personal rights on the web portal. GIODO ordered Company C to reveal the IP address of the user on the grounds that, pursuant to the Act, the processing of personal data (revealing the IP Address) may take place without consent if it is necessary to pursue the legitimate purpose of a data receiver, and this will not violate the rights and freedoms of the data subject. In this case the legitimate purpose was the protection of the individual's personal rights.	Company C filed a complaint against GIODO's decision to the Regional Administrative Court, arguing that 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. In addition, Company C argued that the individual may pursue his claims of infringement of his personal rights through civil or criminal proceedings. The court upheld GIODO's decision, repeating GIODO's reasoning. Moreover, the court held that the Act on Rendering Electronic Services does not prejudice the application of the Act. The court also stated that without the IP address of the user the individual will be not able to pursue his claim in civil proceedings because it is obligatory to identify the infringer in the statement of claims.
17 July 2013 (II SA/Wa 815/13)	The court	An individual requested GIODO to determine whether the court carrying out criminal proceedings against the individual was processing their personal data in violation of the law. In addition, the individual requested GIODO to order the court to remove the data which were in violation of the law. GIODO rejected the request, holding that the violation of the law was minor and incidental. Moreover, GIODO stated that it has no authority to determine whether the decisions issued by the court are null and void, even if, in the proceedings leading to the decision, personal data were processed in violation of the law.	The individual filed a complaint against GIODO's decision to the Regional Administrative Court. The Regional Administrative Court upheld the decision partially repeating GIODO's argument. The Regional Administrative Court held that GIODO has no legal obligation to report a violation of the law to the prosecutor on the grounds that it was an obligation from the individual.

Spain

Total number of resolutions	Classification of matters to which infringements refer	Number of resolutions
189 resolutions	Improper inclusion of personal data in a defaulters list	96
	Processing of personal data without consent	36
	Sending commercial communications without consent	23
	Video surveillance	12
	Others resolutions (data inaccuracy; obligation to secrecy; data security; disclosure of personal data without consent; data subject's rights; information right when processing personal data).	22

Some highlighted resolutions

Date	Infringing entity	Details of infringement	Sanction(s) imposed
08 May 2013	Vodafone España, S.A.	According to the SDPA, Google was able to access the personal data of Vodafone's clients (including name, surname, telephone number; and ID number or Passport number), due to the fact that appropriate security measures were not adopted by Vodafone.	The SDPA imposed a **fine of EUR 20,000** due to the infringement of Article 9 of LOPD (security of data).

Date	Infringing entity	Details of infringement	Sanction(s) imposed
06 June 2013	Recobros Extrajudicial, S.L.	The entity sent nine faxes with commercial content to two SDPA fax lines (without having obtained previous express and informed consent).	The SDPA imposed a **fine of EUR 30,000** due to the infringement of Article 38.3.h) of LGT (need for consent to send commercial communications by fax).
25 July 2013	Mundo Cultura Ediciones, S.L.	The data protection policy of the company included a clause allowing them to disclose data to certain companies for commercial communications purposes to the data subject. However, it did not inform of the data subjects of the business sectors the companies belonged to , and of the possibility to opt-out of the processing of data for commercial communications purposes.	The SDPA imposed a **fine of EUR 10,000** due to the infringement of Article 5 of LOPD (information right when processing data).
26 July 2013	Mapfre Tech, S.A.	Clients' personal data (including special categories of data) were accessible from the internet. The SDPA considered that security measures had not been properly implemented by the company.	The SDPA imposed a **fine of EUR 50,000** due to the infringement of Article 9 of LOPD (data security).

Sweden

Date	Infringing entity	Details of infringement	Sanction(s) imposed
05 April 2013	The Swedish Armed Forces ("Försvarsmakten")	The Swedish Armed Forces process personal data in PRIO, an operations management system enabling employees and competence management to have access to an HR-module and ReachMee, a web-based tool for internal and external recruitment. ReachMee is provided as a service by a third party provider.	The Data Inspection Board (the "DIB") ordered the Swedish Armed Forces to: • Fulfil the requirement to voluntarily inform its employees (including non-employees applying for a job via ReachMee) of the processing of their personal data in PRIO and ReachMee. It should be noted that the DIB finds that the information to data subjects concerning ReachMee should include information about their personal data being processed by the third party provider as a processor; and: • Separate or block personal data in PRIO when no longer needed for competence management purposes, usually shortly after the data subject has left his/her employment; and in ReachMee when no longer needed for recruitment purposes, usually shortly after a recruitment matter has been closed. The Swedish Armed Forces should also: • Clarify the purposes of the text-boxes and the possibility of attaching documents in ReachMee for job applicants, with the aim to avoid applicants providing unnecessarily intrusive information; and • Instruct ReachMee users on how to use the note functions in ReachMee, including clarifying the purpose of the note function and what types of information may be registered there, with the aim to counteract employees registering unreasonable or unnecessarily intrusive information in the note function.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
17 April 2013	Unemployment Insurance Fund for Graduates ("Akademikernas arbetslöshetskassa") (the **"AEA"**)	The AEA used several IT-systems to process data relating to its members and the systems were partly integrated with one another. The Swedish Federation of Unemployment Insurance Funds (The **"SO"**) provided the systems and was responsible for their development. The SO was also in charge of the maintenance of a shared platform for information exchange. The maintenance of the other systems, however, was conducted by a third party provider which had entered into a processor agreement with the AEA.	The DIB ordered the AEA to: • Cease the processing of personal data concerning the members' labor union memberships; • Supplement the information given to the members so it would fulfill the demands of sections 23-25 of the PDA; • Take measures to separate personal data that is not needed for day-to-day operations from other data; • Introduce a logging procedure for the systems when the personal data is accessed, and to develop log surveillance routines; • Encrypt any communications with the third party provider that is conducted over open networks. The DIB also assumed that the AEA would: • Produce instructions on the use of text-boxes and procedures to detect and delete information which, for privacy reasons, should not be entered into the boxes; • Cease processing personal data which has not been kept in accordance with archive legislation and which is no longer necessary to processes with consideration of the purposes of the processing; and • Go through with the planned implementation of electronic identification for the authentication of users or similar and equally secure measures of authentication

Date	Infringing entity	Details of infringement	Sanction(s) imposed
17 April 2013	The Management Staff's Unemployment Insurance Fund ("Ledarnas arbetslöshetskassa") The **"Fund"**	The Fund used several IT-systems to process data relating to its members and the systems were partly integrated with one another. The Swedish Federation of Unemployment Insurance Funds (The **"SO"**) provided the systems and was responsible for their development. The SO was also in charge of the maintenance of a shared platform for information exchange. The maintenance of the other systems, however, was conducted by a third party provider which had entered into a processor agreement with the Fund.	The DIB ordered the Fund to: • Cease the processing of personal data concerning the members' labor union memberships; • Supplement the information given to the members so it would fulfill the demands of sections 23-25 of the PDA; • Take measures to separate personal data that is not needed for day-to-day operations from other data; • Introduce a logging procedure for the systems when the personal data is accessed, and to develop log surveillance routines; • Encrypt any communications with the third party provider that is conducted over open networks. The DIB also assumed that the Fund would: • Produce instructions on the use of text-boxes and procedures to detect and delete information which, for privacy reasons, should not be entered into the boxes; • Cease processing personal data which has not been kept in accordance with archive legislation and which is no longer necessary to processes with consideration of the purposes of the processing; and • Go through with the planned implementation of electronic identification for the authentication of users or similar and equally secure measures of authentication

Date	Infringing entity	Details of infringement	Sanction(s) imposed
17 April 2013	The Swedish Federation of Unemployment Insurance Funds ("Arbetslöshetskassornas samorganisation") The **"SO"**	The SO process personal data concerning the members of Swedish unemployment insurance funds. The SO was found to merely provide the systems, and conduct the maintenance of the shared platform for information exchange to the insurance funds. The funds were free to allocate themselves to whichever service provider would handle the maintenance of the other systems.	The DIB found that the SO was not the controller of the processing of personal data concerning the members of the funds. The DIB instead found SO to be the funds' processor when testing the systems and regarding the processing of personal data available through the platform for information exchange which it was in charge of maintaining.
03 May 2013	Söderberg & Partners Insurance Consulting KB **"S&P"**	S&P is an insurance advisor and broker. Employees and customers had access to sensitive personal data via the internet, subject only to authentication by username and password.	The DIB ruled that S&P shall take appropriate actions, meaning that both customer and employee access to sensitive personal data must only be granted subject to strong authentication (i.e. multi-factor authentication). Such strong authentication may include electronic identification and other technical functions for asymmetric encryption and certain solutions for one-time passwords or similar.
03 May 2013	Max Matthiessen AB **"MM"**	MM is an insurance advisor and broker. Employees and customers had access to sensitive personal data via the internet, subject only to authentication by username and password.	The DIB has ruled that MM shall take appropriate actions, meaning that both customer and employee access to sensitive personal data must only be granted subject to strong authentication (i.e. multi-factor authentication). Such strong authentication may include electronic identification and other technical functions for asymmetric encryption and certain solutions for one-time passwords or similar.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
3 May 2013	Cerberus AB **"Cerberus"**	Cerberus is an insurance advisor and broker. Employees and customers had access to sensitive personal data via the internet, subject only to authentication by username and password. It was also found that Cerberus did not organise personal data which is or has been used for direct marketing purposes.	The DIB ruled that Cerberus shall take appropriate actions, meaning that both customer and employee access to sensitive personal data must only be granted subject to strong authentication (i.e. multi factor authentication). Such strong authentication may include electronic identification and other technical functions for asymmetric encryption and certain solutions for one-time passwords or similar. Furthermore, the DIB rules that Cerberus shall organise any personal data which is being processed for direct marketing purposes within three (3) months after the date of collection.
8 May 2013	The Social Welfare Board of Halmstad ("Socialnämnden i Halmstad") The **"Board"**	The DIB investigated the Board's processing of personal data through the use of mobile devices. The Board offered tablets to the members in order to distribute electronic documents before and during meetings. The investigation was made in order to ensure that proper measures had been taken to protect the data through the use of these mobile devices.	The DIB required the Board to : • Develop functions for the safe transfer of sensitive personal data over networks. • Encrypt confidential and sensitive personal data that is stored on mobile devices. • Enable a process of authentication for users in order to gain access to the personal data. The DIB noted that it assumed that the Board will complement its current user instructions in order to comply with the DIB's check-list for the processing of personal data with the use of mobile devices.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
08 May 2013	The Social Welfare Board of Järfälla ("Socialnämnden i Järfälla") The **"Board"**	The DIB investigated the Board's processing of personal data through the use of mobile devices. The Board offered tablets to the members in order to distribute electronic documents before and during meetings. The investigation was made in order to ensure that proper measures had been taken to protect the data through the use of these mobile devices. The Board was yet to process sensitive personal data in the mobile devices but intended to as soon as the security measures had been deemed in accordance with the PDA. In order to make the data accessible through the mobile devices an app is used from a third party provider.	The DIB required the Board to: • Develop written instructions to the users. • Ensure that the log-in process to the user interface had strong authentication standards. • Develop routines for regular log follow-up. • Develop routines dedicated to prohibiting the access to personal data that no longer needed to be available through a mobile unit. • Sign a processor agreement with the third party provider.
08 May 2013	The Social Welfare Board of Norrköping ("Socialnämnden i Norrköping") The **"Board"**	The DIB investigated the Board's processing of personal data through the use of mobile devices. The Board offered tablets to the members in order to distribute electronic documents before and during meetings. The investigation was made in order to ensure that proper measures had been taken to protect the data through the use of these mobile devices.	The DIB required the Board to ensure that the authentication method used complies with high-level authentication standards. The DIB noted that it assumed that the Board will: • Complement its current user instructions in order to comply with the DIB's issued check-list for the processing of personal data with the use of mobile devices; and • Develop routines dedicated to prohibiting the access to personal data that no longer need to be available through a mobile device.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
31 May 2013	The Municipality Board of Salem ("Kommunsstyrelsen i Salem") The **"Municipality"**	The DIB had previously investigated the Municiplaity's use of the cloud computing service "Google Apps", and ordered the Municipality to enter into a processor agreement with the service provider. Following the DIB's investigation into the processor agreement, it was found that the agreement that the Municipality intended to enter into with the cloud computing service provider ("molntjänstleverantör") did not meet the requirements concerning the instructions to be given to the service provider regarding the purpose of the processing and the deletion of the personal data. Furthermore, the agreement did not guarantee the Municipality appropriate knowledge of which subcontractors would be used by the service provider.	The DIB ordered the Council to: • Cease using the cloud services *or* • Take measures to ensure that the instructions given to the service provider meet the demands of the PDA. • Ensure that the Council has knowledge of any subcontractors used by the service provider.
31 May 2013	The Municipality of Umeå ("Umeå kommun") The **"Municipality"**	The Municipality registered personal data on its employees' working capabilities, some of which was sensitive personal data.	DIB found that the registration was allowed, *inter alia,* because it was necessary in order for the Municipality to fulfil its obligations as an employer. However, the DIB points out that the Municipality shall review its procedures for registration of such data so that it is in compliance with the PDA in each individual case. DIB orders the Municipality to: • Review its routines for sorting out/limiting access to such data that is no longer needed for the purpose for which it was collected. • Inform its employees of its personal data processing for employee rehabilitation purposes. DIB assumes that the Municipality takes appropriate organisational and technical measures to protect the personal data.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
17 June 2013	Gårdstensbostäder AB The **"Company"**	The DIB noted that there had been occurrences of unlawful processing of personal data by public housing companies in the Gothenburg area. Data regarding the tenant's health, ethnicity and past criminal charges had been registered by the Company without prior consent being given by the individuals.	The DIB found that: • The Company had processed the sensitive personal data in breach of sections 13 and 21 of the PDA. • The Company's processing of personal data did not comply with section 9 of the PDA as the processing did not meet industry customs ("god sed") according to an industry agreement. As the Company had recently taken measures to prevent the unlawful processing of personal data that had occurred, the DIB decided not to impose any sanctions.
17 June 2013	Göteborgs Stads Bostadsaktiebolag The **"Company"**	The DIB noted that there had been occurrences of unlawful processing of personal data by public housing companies in the Gothenburg area. Data regarding the tenant's health, ethnicity and past criminal charges had been registered by the Company without prior consent being given by the individuals.	The DIB found that: • The Company had processed the sensitive personal data in breach of sections 13 and 21 of the PDA. • The Company's processing of personal data did not comply with section 9 of the PDA as the processing did not meet industry customs ("god sed") according to an industry agreement. As the Company had recently taken measures to prevent the unlawful processing of personal data that had occurred, the DIB decided not to impose any sanctions.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
17 June 2013	Bostads AB Poseidon The **"Company"**	The DIB noted that there had been occurrences of unlawful processing of personal data by public housing companies in the Gothenburg area. Data regarding the tenant's health had been registered by the Company without prior consent being given by the individuals.	The DIB found that: • The Company had processed the sensitive personal data against section 13 of the PDA. • The Company's processing of personal data did not comply with section9 of the PDA as the processing did not meet industry customs ("god sed") according to an industry agreement. As the Company had recently taken measures to prevent the unlawful processing of personal data that had occurred, the DIB decided not to impose any sanctions.
17 June 2013	Familjebostäder i Göteborg AB The **"Company"**	The DIB noted that there had been occurrences of unlawful processing of personal data by public housing companies in the Gothenburg area. Data regarding the tenant's health, ethnicity and past criminal charges had been registered by the Company without prior consent being given by the individuals.	The DIB found that: • The Company had processed the sensitive personal data against section13 and section21 of the PDA. • The Company's processing of personal data did not comply with section9 of the PDA as the processing did not meet industry customs ("god sed") according to an industry agreement. As the Company had recently taken measures to prevent the unlawful processing of personal data that had occurred, the DIB decided not to impose any sanctions.

United Kingdom

Date	Infringing entity	Details of infringement	Sanction(s) imposed
21 May 2013	News Group Newspapers	A server holding part of the Sun Newspaper's website was attacked in July 2011 and large amounts of personal data relating to the Sun's customers was leaked onto the internet. None of the data was sensitive personal data; some of it was several years old. The server in question had not been used for its intended purpose and News Group Newspapers accepted that it had failed to follow its own internal IT governance policies adequately.	News Group Newspapers undertook to: • Ensure that all its staff are aware of its policy for the storage and use of personal data and are appropriately trained in how to follow that policy; • Improve technical security controls to prevent further unauthorised access to personal data via its web servers; • Regularly monitor compliance with data protection and IT security policies; • Implement measures to ensure that any customer data collected as part of its activities is regularly cleared in line with a defined retention and disposal policy; and • Implement additional security measures to ensure that personal data is protected against unauthorised or unlawful processing, loss, destruction or damage.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
23 May 2013	Paul Hedges	Mr Hedges was the former manager of a council-run leisure centre in Southampton. His prosecution related to his unlawful obtaining of sensitive medical data relating to over 2000 users of the leisure centre. Mr Hedges was intending to use the data for a new business venture. After he was made redundant by the leisure centre, Mr Hedges emailed the information to his personal email account, as he was intending to set up a new fitness company. The information resulted from the Council's Active Options GP referral service, where patients would be referred by their GP or other health professional to attend fitness sessions. The council was made aware of Mr Hedges' actions after users of the leisure centre reported being contacted by Mr Hedges to join his new fitness service.	Mr Hedges was prosecuted at West Hampshire Magistrates court. He was convicted under s55 of the DPA for unlawfully obtaining sensitive medical data. Mr Hedges was fined £3,000 and required to pay £1,376 towards the costs of prosecution. He was also told to pay a £15 victims' surcharge.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
31 May 2013	Leeds City Council	The ICO conducted a follow-up investigation of Leeds City Council, following an undertaking given on 28 November 2012, to ensure that Leeds City Council had complied with the requirements in the undertaking which it gave in November 2012. The ICO's review concluded that Leeds City Council had taken the appropriate steps and put plans in place in order to comply with the undertaking, but the planned work needs to be completed before the Council is fully compliant with its previous undertaking.	The ICO concluded that Leeds City Council still needs to: • Continue to develop its "Transforming Procurement Programme", which will incorporare monitoring arrangements into its strengthened and formalised procurement process. Once the Programme is implemented, the Council should monitor its progress to ensure that data protection requirements are met; and • Ensure that scheduled work relating to IT governance training and secure file transfers is completed.
31 May 2013	Prospect	The ICO has conducted a review into whether Prospect had met the requirements of the undertaking which it gave on 8 January 2013. The ICO found that Prospect had taken some steps and put plans in place to comply with the undertaking, but there was further work to be done.	The ICO has recommended that Prospect takes the following actions: • Complete its review of its data protection policies as soon as possible and introduce an information security policy as previously recommended; • Provide annual refresher training to its staff; and • Implement the recommendations from its independent data security review.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
03 June 2013	Stockport Primary Care Trust	The data controller was found to have left behind boxes containing confidential and highly sensitive personal data relating to over 200 data subjects at a decommissioned site. The ICO's review concluded that the data controller had failed to take appropriate organisational measures, such as having a decommissioning policy. The ICO also considered that the existing measures did not ensure a high level of security, with the breach likely to cause substantial distress.	A monetary penalty of £100,000 was issued by the ICO.
05 June 2013	Halton Borough Council	A clerical officer working in the data controller's administrative service, while sending a letter from the adoptive parents to the birth mother, accidently included the address of the adoptive parents. This led to the birth mother's parents getting in touch with the adoptive parents, followed by an unsuccessful Court application for the right to direct contact with the child. The ICO report found a serious contravention of section 4 (4) of the Data Protection Act through the data controller's failure to take appropriate organisational measures against the processing of personal data. This was compounded by the fact that the data subjects suffered substantial distress from the breach, following inappropriate contact from the unauthorised third parties. Furthermore, the ICO took into account the fact that one of the data subjects in question was a vulnerable child.	A monetary penalty of £70,000 was issued by the ICO.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
07 June 2013	Glasgow City Council	The ICO has served an enforcement notice on Glasgow City Council following the theft of two unencrypted laptops from the councils' offices, one of which contained the personal information of 20,143 people. There had been previous thefts of equipment from these offices but physical security measures had not been improved. 70 other unencrypted laptops were also unaccounted for. A monetary penalty of £150,000 was issued by the ICO.	The Council has been ordered to: • Conduct a full audit of IT assets used to process personal data by 30 June 2013; • Create a new asset register by 31 July 2013; • Maintain that the register is up to date on a yearly basis; • Provide training to managers in relation to asset management by 30 June 2013; and • Reissue information on security guidelines and update information security training for all staff by 30 June 2013.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
11 June 2013	Google Inc.	In 2010, the Information Commissioner's Office became aware that the data controller's Street View vehicles had mistakenly collected personal data relating to thousands of individuals. This information included email addresses, URLs and passwords. An undertaking was entered into by Google to delete all payload data collected in the UK which the data controller had no outstanding legal obligation to retain. Following this, in 2012, the data controller reported that they had accidently retained five discs which contained payload data collected in the UK.	The ICO issued an enforcement notice, with the data controller to: • Securely destroy within thirty-five days, any personal data held on vehicles discs and collected in the UK using Street View vehicles; and • Promptly inform the Information Commissioner should they discover a Street View vehicle disc holding personal data collected in the UK.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
12 June 2013	Central Bedfordshire Council	An individual's sensitive personal data had been made publicly accessible without consent via a planning portal on the Council's website. The data controller also reported the inappropriate obtaining and use of sensitive personal data held in a social care database by two employees. Central Bedfordshire Council undertook to ensure that that the procedures covering the preparation of planning application documentation for publication would be followed by staff and that all legacy data from the previous authority would be removed by 31 March 2013.	The data controller undertakes to ensure that: • The procedures covering the preparation of planning application documentation for publication are followed by staff; • Staff are aware of the data controller's procedures for the preparation of planning application documentation for publication and are appropriately trained how to follow those procedures; • By 31 March 2013 the social care database referred to in this undertaking contains a completely cleansed dataset free from unnecessary legacy data originating from the previous local authority; and • The data controller shall 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
12 June 2013	Bedford Borough Council	A social care record, containing sensitive personal data, was inherited by two new unitary local authorities from the previous authority's social care database. This record had been compromised by the inappropriate actions of two of its employees. As a result both new unitary authorities inherited records not relevant to their provision of social care services. Bedford Borough Council undertook that all legacy data from the previous authority would be removed by 31 March 2013.	The data controller undertakes to ensure that: • By 31 March 2013 the social care database referred to in this undertaking contains a completely cleansed dataset free from unnecessary legacy data originating from the previous local authority; and • The data controller shall 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.
13 June 2013	North Staffordshire Combined Healthcare NHS Trust	The data controller sent several faxes containing sensitive personal data about vulnerable adults to a member of the public in error. The faxes were intended for a Wellbeing Centre which provides psychological therapies. The ICO report found a serious contravention of section 4(4) of the Data Protection Act through a failure to ensure a level of security appropriate to the harm that might result from such unauthorised processing and the inappropriate organisational measures taken by the data controller.	A monetary penalty of £55,000 was issued by the ICO.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
18 June 2013	Nationwide Energy Services & We Claim You Gain	Both companies are part of Save Britain Money Limited and were found to be responsible for over 2,700 complaints to the Telephone Preference Service or reports to the ICO over a 19 month period from May 2011 for direct marketing. The ICO found these activities to be a breach of Regulation 21 of the Privacy and Electronic Communications Regulations (PECR) on numerous grounds but particularly noted that both companies ignored recognised industry practices to avoid breaches of PECR and showed complete disregard for the requirements of the law.	Monetary penalties of £125,000 and £100,000 were issued by the ICO to Nationwide Energy Services and We Claim You Gain respectively.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
08 July 2013	Tameside Energy Services Ltd	The ICO received over 1,000 complaints between May 2011 and January 2013 regarding unwarranted marketing calls received from Manchester-based Tameside Energy Services Limited. Tameside Energy also failed to update its lists and continued to call people who were registered with the Telephone Preference Service (TPS), thereby breaching the Privacy and Electronic Communications Regulations (PECR). ICO decided that the case met the 'seriousness threshold' under section 55 (1)(a) of the PECR because of the nature, duration and extent of the breach. ICO also decided that the contravention was of a kind that was likely to cause substantial damage or substantial distress under section 55(1)(b) PECR.	Monetary penalty of £45,000 reduced from £90,000 due to the company's financial situation. An enforcement notice was also issued, stipulating that Tameside will: *Neither use, nor instigate the use of a public electronic communications service for the purposes of making unsolicited calls for direct marketing purposes where the called line is that of:* *a) a subscriber who has previously notified Tameside that such calls should not be made on that line; and /or* *b) a subscriber who has registered their number with the TPS at least 28 days previously and who has not notified Tameside that they do not object to such calls being made*

Date	Infringing entity	Details of infringement	Sanction(s) imposed
12 July 2013	NHS Surrey	Computer equipment previously belonging to the data controller was found to contain sensitive personal data belonging to over 3,000 patients. The computers were sent to a third party company for the data to be erased before the equipment could be re-sold via an online auction site. The data controller had no contract in place with the third party and also failed to monitor the data destruction process.	Monetary penalty of £200,000
16 July 2013	Janet Thomas	The website www.janetpage.com, is a specialist recruitment site for the Health Care Profession. A breach of security allowed CVs to be accessible to anyone using the website. This affected approximately 7,435 CVs. The controller suggested that the breach was the result of a dissatisfied applicant who hacked the website, however, no technical proof was provided to support this.	Janet Thomas to: • Review current practices to ensure compliance with the Act and in particular: • Ensure personal data should only be collected when necessary. Consideration should be made as to the type of data collected and all information should be securely disposed of when no longer required.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
26 July 2013	Derbyshire, Leicestershire and Nottinghamshire Police Forces	The forces had been working on a collaborative project, A burglary led to the theft of eight laptops containing (among other things) sensitive personal data including prison records and offender details relating to approximately 4,500 individuals. The laptops were not securely locked away, nor were they encrypted. The data controllers did not carry out a risk assessment before they allowed their officers to join the collaboration and instead relied upon one of the force's security measures, which did not specify encryption or secure storage for laptops. The data controllers did not monitor the officers whilst they were on this secondment for the collaboration.	The three police forces must not share personal data as part of collaborative working initiatives unless: • A Senior Information Risk Owner ("SIRO") has been appointed at the beginning of the collaborative project to oversee work; • The SIRO has risk assessed the vulnerability of premises to burglary and theft at the beginning of any collaborative project and has ensured appropriate security measures are taken to protect personal data; • Laptop computers or other portable electronic storage devices or removable media used by officers working on collaboration projects are encrypted to protect any personal data processed on such devices; • All such officers have received training on the security requirements of the Data Protection Act 1998.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
13 August 2013	Foyles Women's Aid	A support worker left a folder containing sensitive and confidential client information in a café. The ICO found a lack of effective controls and procedures for taking information out of the office. The support worker was also transporting excessive information, as the lost folder contained personal data which was not relevant to the meetings scheduled that day	Foyles Women's Aid to ensure that: • It drafts and implements a policy covering the storage, physical security, transportation, use, and disposal of personal data outside of the office environment and staff to be appropriately trained on the policy; • Compliance with the policies to be appropriately and regularly monitored; • Portable and mobile devices used to store and transmit personal data, the loss of which could cause damage or distress, to be encrypted; and • Physical security measures to be adequate to prevent unauthorised access to personal data.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
13 August 2013	Northern Health and Social Care Trust	A number of security incidents led to a formal investigation. Examples mentioned were confidential information being faxed to a local business and sensitive data being shared with business partners in error. The investigation revealed that despite the data controller having introduced Information Governance training, the majority of staff had not received training. There was a damaging failure to monitor and enforce completion of training.	NHDCT to ensure that: • Sufficient measures are put in place to ensure that all staff attend mandatory training; • Portable and mobile devices used to store and transmit personal data, the loss of which could cause damage or distress, are encrypted; and • Procedures are put in place to ensure any reported breach of security is acted upon promptly and remedial measures enforced. Where necessary staff should receive appropriate additional training and support in this respect

Date	Infringing entity	Details of infringement	Sanction(s) imposed
13 August 2013	Northern Health and Social Care Trust	A number of security incidents led to a formal investigation. Examples mentioned were confidential information being faxed to a local business and sensitive data being shared with business partners in error. The investigation revealed that despite the data controller having introduced Information Governance training, the majority of staff had not received training. There was a damaging failure to monitor and enforce completion of training.	NHDCT to ensure that: • Sufficient measures are put in place to ensure that all staff attend mandatory training; • Portable and mobile devices used to store and transmit personal data, the loss of which could cause damage or distress, are encrypted; and • Procedures are put in place to ensure any reported breach of security is acted upon promptly and remedial measures enforced. Where necessary staff should receive appropriate additional training and support in this respect
15 August 2013	Victoria Idowu	A probation officer incorrectly revealed a domestic abuse victim's new address to the alleged perpetrator. Following this breach, the distressed victim cut off all ties with the police other services and the investigation was subsequently dropped. The probation officer has also been the subject of disciplinary proceedings by London Probation Trust, which resulted in her employment being terminated due to gross misconduct.	Fine of £150 plus £20 victim surcharge and a £250 contribution towards costs.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
22 August 2013	Local Government Ombudsman (LGO)	The theft of a bag containing an encrypted portable media device and hard copy papers relating to complaints made to the LGO. The papers contained sensitive personal data relating to a complainant. Data protection training was considered insufficient to ensure staff awareness of data protection policies and procedures.	LGO to ensure that: • Mandatory induction and annual refresher training to be provided to all staff whose role involves the routine processing of personal data; • Training to be recorded and monitored with oversight at senior level against agreed. LGO to implement follow-up procedures to ensure that staff who have not attended/completed training do so as soon as is practicable; and • Staff to be are aware of the content and location of policies and procedures relating to the use of personal data. A mechanism to ensure that staff are updated of any changes to these policies and procedures should also be implemented.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
23 August 2013	Islington Borough Council	Personal details of over 2,000 residents were released online. The data released included sensitive personal data relating to residents' housing needs, including details of whether they had a history of mental illness or had been a victim of domestic abuse. The data was released in response to a freedom of information request made through the What Do They Know (WDTK) website, which enables individuals to submit requests for information to public authorities. Responses are uploaded to the site and are available to all those wishing to view them. The data controller mistakenly released three spreadsheets containing the data and remained on the website for over two weeks. The data controller had been alerted to the problem shortly after the first spreadsheet was published, but failed to correct the error. This resulted in the other two spreadsheets being released with the same problem.	Monetary penalty of £70,000

Date	Infringing entity	Details of infringement	Sanction(s) imposed
29 August 2013	Aberdeen City Council	Thirty-nine pages of personal data were uploaded onto the internet by a Council employee, following inadequate homeworking arrangements. The sensitive information related to social services and included details relating to the care of vulnerable children and details of alleged criminal offences. The files were uploaded between 8 and 14 November 2011 and remained available online until 15 February 2012. The council had no relevant home working policy in place for staff and did not have sufficient measures to restrict the downloading of sensitive information from the council's network.	Monetary penalty of £100,000

Date	Infringing entity	Details of infringement	Sanction(s) imposed
29 August 2013	Cardiff City Council	Following the failure to respond to a subject access request within the forty day deadline, the data controller's compliance procedures were investigated by the ICO. ICO found systematic failures to meet requirements.	CCC to ensure that: • Procedures are clearly defined and managed, and all staff involved in such work receive appropriate training in how to follow them; • Appropriate checks and supervision are put in place to ensure that third-party data is dealt with in accordance with the Act's requirements and the data controller's policies and procedures; and • Sufficient measures are in place for the storage of paper records to ensure that subject access requests are responded to appropriately.

European data protection news

Drones: Privacy implications across the EU

Gabriel Voisin, Associate, Bird & Bird (London)

Drones have become notorious through their military use. However, industry has now started to look at the civilian applications of drones. While they come in a variety of shapes and sizes, the key element of a drone it that it is an unmanned aerial vehicle ("UAV").

Some of these are piloted remotely and are generally known as Remotely Piloted Air Systems ("RPAS"), whereas others fly autonomously following pre-programmed flight paths. They are generally cheaper to produce than conventional manned aircraft, can be kept airborne for extended periods of time, and do not risk the lives of the crew which pilots them. For the following article, we will collectively refer to them as "Drones".

The use of Drones is extending beyond the military into a number of other sectors, for instance:

- Journalism – Drones can be used to capture footage (e.g. TV companies used Drones to film areas that were inaccessible to film crews after the passage of hurricane Katrina).
- Scientific research – Drones can be fitted with a variety of sensory equipment and can be used to conduct research in conditions inhospitable to humans or for length periods which humans could not endure (see illustration);
- Agriculture – Drones can be used to administer phytosanitary treatments on plantations;
- Advertisement – Drones can be used to tow banners across the sky; or
- Surveillance by law enforcement agencies or private companies – Surveillance is already a major use of Drones in the military and the same technology could be applied to commercial use. They are even being used by Paparazzi as this article on Der Spiegel demonstrates;

- In 2012, the US passed a law allowing the Federal Aviation Administration (FAA) to authorise government agencies and law enforcement to use Drones, and it has to start allowing commercial use of Drones by 2015.

In the Europe Union, use of Drones raises legal questions. The following three possible legal issues can be identified:

- Aviation regulations regarding the use of Drones;
- Data protection implications where the Drone is capturing personal data; and
- CCTV regulations where domestic law would regard video capture by Drones as equivalent to CCTV.

The table below briefly summarise the law in regard to each of these issues for the various European jurisdictions in which Bird & Bird are based:

Country	Aviation Requirements	Data Protection Requirements	CCTV Requirements
Belgium	YES – Drones used for recreational purposes are subject to the following provisions: • Use of Drones: Decree of 15 September 1994 on air traffic rules; C.A.A. measure of 1 June 2005 ("Circulaire") CIR/GDF-01. • Manufacturing of Drones: no specific rule (possible application of the Toys Safety Act of 9 February 1994 to the manufacturing of Drones sold for recreational purposes). The use of Drones in Belgian airspace is subject to an authorization being obtained from the Belgian C.A.A. and from the Belgian Telecommunications Institute (IBPT).	POSSIBLY – The use of a Drone to capture or record images of individuals for the purpose of surveillance in a public open space (e.g. a park) or in a private space open to the public (e.g. a shop) is prohibited, except if use by law enforcements bodies (Camera Surveillance Act of 21 March 2007). Belgian data protection law applies to the capture of images with no surveillance purpose: a valid ground for processing data would be needed (e.g. legitimate interest of the controller), information should be given to the data subjects, and the Belgian Data Protection Agency would have to be notified of the data processing activity.	The use of Drones for CCTV purposes is prohibited except if use by law enforcements bodies.

Country	Aviation Requirements	Data Protection Requirements	CCTV Requirements
France	YES – Drones are subject to the following regulations: • Use of Drones: Decree of 11 April 2012 • Manufacturing of Drones: Decree of 11 April 2012 If a device recording any type of data from outside the visible spectrum (e.g. radar, thermograph, infrared) is used by a Drone, authorisation is required. This authorisation is valid for no more than 3 years. If a device recording any type of data from within the visible spectrum (e.g. photographs and videos taken from an image/video recording device/camera) is used by a Drone, then a declaration shall be done two weeks before the operations take place, unless the Drone is deployed for recreational use on an occasional basis.	POSSIBLY – If a Drone captures and records images of individuals, French data protection law would apply: a valid ground for processing data would be needed (e.g. legitimate interest of the controller), information should be given to the data subjects, and French Data Protection Agency would have to be notified of the data processing activity. The notification requirement would be satisfied by way of a filing which specifies the purpose of the activity, the categories of personal data processed, the data subjects, the recipients to whom the personal data may be disclosed and the retention period of personal data. The notification is valid for an unlimited period of time. Note that the CNIL has issued a public statement on this issue which can be found here (in French).	POSSIBLY - If CCTV is used by a Drone to monitor places open to the public (e.g.: amusement park), an authorization from the police headquarters ("Prefecture de Police") would also be needed. The authorization is valid for 5 years and will have to be renewed before expiration. The above applies even if the images are not recorded. Note that we are not aware of any police authorisation having been issued in this respect. Like for the UK, the public notice requirement is likely to be difficult to satisfy.

Country	Aviation Requirements	Data Protection Requirements	CCTV Requirements
Germany	YES – Drones are subject to the following regulations: • German Air Trafic Act ("Luftverkehrsgesetz"); and • German Aviation Regulation ("Luftverkehrs-Ordnung" – "GAR") According to s. 15 a para.3 GAR the use of Drones which are not operated for sports or recreational purposes, is generally prohibited if the Drone is used: (i) out of sight of the controller; or (ii) the total mass of the device is more than 25 kilograms. However, it is – as an exception to this rule – possible to obtain an authorization to use Drones from the competent local Aerial Authority. Such a license will only be granted if the intended use does not constitute a risk to public order and security (and in particular does not infringe on personal rights of individuals and, accordingly, German data protection law).	POSSIBLY - There are no specific data protection regulations which apply to Drones, nor any specific guidance on the subject. However, it is conceivable that certain data gathered by Drones could be considered personal data (in particular if images of individuals are captured/recorded), in which case the data would have to be processed in accordance with the German Data Protection Act ("Bundesdatenschutzgesetz" – "GDPA"). In this context it should also be noted that an authorization (cf. left column) will only be granted if the user declares that the use of Drones does not infringe data protection law.	YES – According to s. 6 b GDPA, CCTV, if used by a Drone to monitor places open to the public, is only lawful as far as: (1) necessary for: (i) public bodies to perform their duties; (ii) to exercise the right to determine who shall be allowed or denied access; or (iii) to pursue legitimate interests for specifically defined purposes; and (2) there are no indications of overriding legitimate interests on the part of the subject of the data. The specific information obligations required by German data protection law (i.e. providing the public notice of the CCTV system) might be difficult to implement when Drones are being used. The monitoring of dwellings and other spaces especially protected from view (e.g. a hedge-protected garden) is prohibited under section 201 a of the German Criminal Code ("Strafgesetzbuch"). Such monitoring requires the individual's consent.

Country	Aviation Requirements	Data Protection Requirements	CCTV Requirements
Spain	POSSIBLY – Civil applications are yet to be developed and currently Drones are only used for experimental purposes. For the time being under Spanish legislation, Drones may only obtain authorisation from the Spanish Civil Aviation General Directorate to operate for experimental purposes under a Special Experimental Certificate of Airworthiness or ("Certificado de Aeronavegabilidad Especial Experimental"). A regulatory framework for the civilian applications of Drones is expected to be developed in the near future, jointly by the Spanish Civil Aviation authority together with the Spanish National Security Aviation Agency ("AESA").	POSSIBLY – Use of Drones are not foreseen in the Spanish Data Protection Act. However, personal data collected through Drones would have to comply with Spanish data protections law: a valid ground for processing data would be needed (e.g. legitimate interest of the controller), information should be given to the data subjects and the Spanish Data Protection Agency would have to be notified of the data processing activity. Please note that data protection regulations are not applicable to images obtained by the media.	POSSIBLY – CCTV requirements are regulated by Data Protection regulations. Certain obligations regarding information requirements would be difficult to comply with. Images obtained by private entities must comply with the data quality principle and avoid all unnecessary images of public spaces. Images of public spaces obtained by the police need an administrative authorization. Regarding sports events, there are specific regulations that foresee the use of mobile cameras (non-fixed) for security reasons. Drones are not mentioned specifically in these regulations, but they may serve as a legal ground to use them.
UK	YES – The Civil Aviation Authority (the CAA) has published detailed guidance covering the regulation of Drones in the UK. Drones operating in the UK must meet at least the same safety and operational standards as manned aircraft (the specific requirements vary with the size of the aircraft).	POSSIBLY - There are no specific data protection regulations which apply to Drones, nor any specific guidance on the subject. However, personal data collected through Drones would have to comply with the Data Protection Act: a valid ground for processing data would be needed (e.g. legitimate interest of the controller), information should be given to the data subjects, and the UK Data Protection Agency would have to be notified of the data processing activity.	POSSIBLY - There is no specific legal regime relating to CCTV in the UK. However, the Data Protection Act does apply to CCTV systems. The ICO would have to be notified of the data processing. Certain obligations regarding providing the public notice of the CCTV system might be difficult to implement when Drones are being used. This problem was mentioned by the ICO in their submission to the Joint Committee - pre-legislative scrutiny of the draft Communications Data Bill (at page 55).

As outlined above, each country concerned will have its own set of issues and legal restrictions to be considered before Drones can be used. One of the main difficulties is around the duty to inform individuals subject to Drone activities.

Theoretically, under EU and Member State laws, Drone controllers must provide individuals with information about data processing. However, this does not apply when individuals have already been informed, or when informing them proves impossible or would involve disproportionate efforts. Drone controllers could benefit from this exemption.

However, they will still have to engage in general information campaigns in an adequate way. As Google did with its Google Street View service, Drone controllers could arrange a dedicated and visible section of their websites to inform the public of their activities. The notice would have to contain the following information: details of the entity responsible for processing Drone data; purposes of processing; the type of data; the duration of processing; the rights of data subjects to access, rectify or erase their data and the right to object.

It should also be noted that Drones are being viewed as a growing concern by individuals and part of the civil society. As a result, industry and entrepreneurs have started looking at ways to circumvent Drone technologies. For example, recently a New York based entrepreneur introduced a line of 'anti-drone' clothing intended to thwart aerial surveillance, in particular thermal imaging. This work highlights the growing unease felt on the ground at the possibility of the sky swelling with new surveillance technologies, such as Drones.

France

Reduction of damages awarded for unpermitted use of client data: a direct consequence of the victim's insufficient security measures

Gabriel Voisin, Associate, Bird & Bird (London)

In this case, a French e-commerce operator noticed that its client list, containing the email addresses of 4.7 million clients and prospects, was compromised. It noticed this once advertisements from a competitor started being received by fictitious email addresses, set-up purposely to alert the e-commerce operator of any security breaches. The competitor admitted to obtaining the client list from an employee of the e-commerce operator. The employee used her credentials, which were also being used by four other employees, to access the information. The client list was used by the competitor on several occasions for duration of three months. He also shared part of the list with advertising agencies for different publicity campaigns.

The Tribunal de Grande Instance ("TGI") of Paris handed down a judgment proclaiming the competitor's liability for appropriation, unbeknownst to the e-commerce platform, of client and prospective client email addresses, for personal gains. The TGI also considered that the advertising agencies were negligent in acquiring client list information at a very generous price without questioning the conditions in which the seller had itself acquired the information. According to the TGI, this price, too weak to permit an injection of investment which is required for the creation and maintenance of such a large client list, ought to have alerted the advertising agencies to the dubious origins of the information.

Subsequently, the e-commerce platform successfully obtained the conviction of the competitor and the advertising agencies. However, the TGI deemed the e-commerce platform to be responsible for 30% of the damages it incurred as a result of the absence of firm rules on client database access. Without explicitly quoting the security obligations laid down by the French Data Protection Act, the TGI sanctioned the plaintiff for its lack of security measures in the management of the credentials.

The e-commerce platform claimed that it implemented several measures to ensure the security of its client list including (i) the use of fictitious email addresses to identify improper use of client data; (ii) the implementation of confidentiality obligations in the contracts of the e-commerce platform employees; (iii) the use of credentials to access the client database; (iv) logging accesses to the information; (v) the provision of security services by exterior companies; and (v) the development of perfected IT and technical infrastructure.

Unfortunately, this was deemed insufficient by the TGI. According to the TGI, the fact that the credentials used by the unfaithful employee were also being utilised by four different individuals within the company, including a designer (who, at first-glance, had no need to access the information, noted the TGI), demonstrated a degree of negligence in the management of credentials attributable to the e-commerce platform. Consequently, it was deemed that the e-commerce platform contributed to the damages it incurred by 30% as a result of not implementing appropriate security measures on the management of credentials giving access to personal data of clients and prospects. It followed that €30,000 would be subtracted from the €100,000 of damages that the plaintiff was awarded.

Take away from this court decision: (i) companies must ensure that they satisfy their security obligations: insufficient or a lack of security measures expose them to reduced damages or denial of damages in case of improper use of data by third parties; and (ii) list vendors must be very cautious when acquiring client list information: very generous prices should raise questions. A copy of the court decision (in French) can be found here.

Italy

Data protection update on recent Garante decisions, authorities and guidance

Debora Stella, Avvocato, and Gianluca Agostinis, Trainee, Bird & Bird (Milan)

Video surveillance

The proportionality principle in art. 11 of the Italian Data Protection Code requires that in case of CCTV systems with recording cameras, the retention of images has to be proportionate to the time required to achieve the specific purpose(s).

Generally, the images can be retained for up to a maximum of 24 hours, subject to special requirements whereby the images can be retained for longer due to festivities and/ or; following specific requests by investigating judicial and police authorities.

However, it is important to highlight that the Italian DPA has recently adopted some new decisions providing for longer retention periods of the images in cases of particular high-risk activities:

- Decision February 7, 2013: The Italian DPA authorised a retention period of **30 days** for a company that operates the international transportation of goods and custom barrier services, due to the need to comply with the voluntary certification TPAT.

- Decision March 7, 2013: The Italian DPA authorised a retention period of **12 months** for a company producing paper money to be used to print Euro banknotes. The extended retention period was justified by security requirements imposed by the European Central Bank.

- Decision April 11, 2013: The Italian DPA authorised a retention period of **14 days** for the National Agency for new technologies, energy and economic sustainable development (ENEA) due to the particularly sensitive nature of the Agency's activities.

- Decision June 6, 2013: The Italian DPA authorised a retention period of **30 days** for a company delivering postal mail and parcels.

Profiling data

In two recent decisions, the Italian DPA authorised the luxury fashion brands Salvatore Ferragamo (decision dated 30 May 2013) and Bulgari (decision dated 24 April 2013) to retain profiling data for periods longer than the ordinary maximum period of 12 months.

The Italian DPA authorised the companies to retain profiling data - related to customers who expressly and actively consented to profiling operations - **respectively**, for **7 and 10 years.** This is based on the consideration that the frequency of contacts and purchases in the fashion sector is definitely lower (average of 2 purchases for each customer during one year) than in others sectors such as the telecommunications or food and beverage industry; and a longer retention period is considered to be legitimate in addressing this.

Banking data

In the decision dated 18 July 2013, the Italian DPA provided clarifications of decision n. 192/2011, regarding the "Circulation of clients' personal data among a bank group and traceability of bank transactions", which containing the following main obligations:

a) The company outsourcer, which carries out the processing of data according to the instructions of the bank (i.e. the real data controller), has to be appointed as the data processor;

b) All bank transactions (i.e. any order and/or consultation of information concerning the economic and financial situation of a bank account holder) must be traced using an appropriate method of log-in identification (this tracking covers all persons in charge of the processing, i.e. "incaricati del trattamento");

c) These traceable log-ins have to be retained for at least 24 months;

d) The banks have to deliver specific alerts in case of any irregular events;

e) The banks have to arrange an internal audit assessment, on an annual basis at least

The new decision clarified several points raised by the Italian Bank Association (ABI) in properly identifying the boundaries of these security obligations:

- "**Bank transaction**" means those operations regarding banking activity in the strictest sense of the word, thereby relating to the gathering of savings from the public and providing loans. The term also includes "any financial activity" eligible for mutual recognition, including all the activities that can be carried on by all the banks operating inside the European Union on the mutual recognition basis;

- "**Bank information**" means any information contained within the statements of an account, information concerning bank transactions, active and passive transactions on the bank account, and the transactions requested by the account holder relating to the contractual relationship

- In case of increased access to the account holders' data, the information to be collected in relation to the "incaricato", who carried out the query are; the date, time, details of the query, and whether the query covered multiple individuals or accounts.

Finally, the authority postponed the deadline to comply with these security measures to 03 June 2014.

Direct marketing

In the general decision dated 15 May 2013, the Italian DPA simplified the way controllers must implement measures to collect valid consent for direct marketing activities.

In particular, the Italian DPA stated that all private data controllers who have obtained specific consent, according art. 130 of the Code, for direct marketing activities carried out through automated means and electronic communications; are entitled to carry out marketing activities and can also implement the same data processing through traditional systems such as postal mails or calls made by an operator, without the requirement to obtain further consent from the data subject. This is subject to the data subject in question not having exercised the right of opposition to the processing.

In order to do so, it is necessary that in the information notice and request of consent, it is clarified that the promotional communication will be sent not only through computer-based systems, but also via traditional channels (e.g. postal mail), and that the data subject will always be able to oppose to these communications or indicate a preferred channel.

Spamming activities

The Italian DPA issued another general decision, dated 04 July 2013 (a summary of which is available in English here: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2554512), which is strictly connected to the aforementioned case on promotional activities.

This decision partially revises a previous decision of the authority on the same matter issued in 2003, and is intended to emphasise (and in some cases, clarify) what the requirements to ensure compliance with the legislation when performing marketing activities, primarily through electronic systems are.

- "Spamming" is clarified by the Italian DPA as any activity consisting of the sending of advertising material for direct marketing, commercial communication or for market research purposes made in violation of the provisions of the Data Protection Code through electronic systems and this applies irrespective of the number of e-mails sent out for such purposes. Therefore, only one e-mail is sufficient to breach the law.

- Legal entities and associations still remain subject to the rules concerning marketing through electronic systems.

- An information notice on the processing of personal data for marketing purposes must be given in advance of the processing; and it must clearly contain, *inter alia*, the recipients in case of disclosure of data, the modalities used to process the data (including whether the communications will be sent via traditional mail or by e-mails, SMS, etc.); and all purposes for which their data will be processed. In case of data collected through third parties, the notice will include the kind of data processed by the controller; and shall be given to the data subject upon registration of the information or on its disclosure to third parties.

- Consent:
  - Opt-in is required for pre-recorded calls, e-mails, faxes, SMS or MMS, and similar.

  - Opt-out is only allowed in the customer/vendor relationship provided that:

(i) the customer is informed of such processing and is offered the chance to opt-out initially, and in any following communications; and
(ii) the promotion concerns goods or services that are similar to those that have already been purchased and are from the same controller that initially collected the e-mail/postal addresses;

- It is sufficient to obtain one single consent for:

(i) all the processing that falls under the wide definition of "marketing activities". This includes sending ads and/or performing market surveys, but not profiling or targeting activities, for which separate consent is required; and
(ii) whatever channel of communication is used (physical address and phone calls with operators or electronic contacts), provided that the user is informed that it is entitled to object to each single channel of communication;

- However, such consent cannot also cover the marketing activities independently carried out by third parties: if a company plans to collect users' personal data to disclose or transfer such data/database to third parties for their independent promotional purposes, the company must obtain a separate and additional consent;

- Consent is only validly obtained when it is free, specific, informed and recorded in writing. Therefore, consent is to be separate from the Terms and Conditions and customers cannot be forced to agree, so it is also unlawful if consent to marketing activities is a precondition to register to a website and/or the check box is pre-ticked;
- It is not possible to send commercial offers without prior consent, even if the personal data has been extracted from public registers, lists, institutional websites or documents that can be publicly accessed.

- Specific anti-spamming solutions must be used by the service providers.

- In case of any contracting (and sub-contracting) the marketing activities, the controller must also appoint the sub-contractors as data processors;

- Unsolicited marketing faxes may be subject to the Data Protection Code even if the fax is sent from other EU countries;

- Just because data happens to be available on the network does not mean that it may be used freely to send automated promotional messages or for any other "viral" or "targeted" marketing purposes. Regarding the so called "social spam", any commercial message posted privately on the board of the user of a SNS (Social Networking Site) is subject to the prior consent of the user. However, in case of users who become “fans” of a page or a company or subscribe to a group of “followers” of a certain brand, VIP, product, etc., the company may send promotional messages to its “fan” or “followers” on the SNS if it appears that the users are unambiguously interested in receiving commercial communications about such product, brand, company, VIP, etc., based on information available at the time of registration

Disaster recovery (and cloud services) for Public Administrations

In the decision dated 04 July 2013, the Italian DPA gave its opinion on the draft "Linee-guida per il Disaster Recovery delle pubbliche amministrazioni" (Guidelines for the Disaster Recovery of Public Administration), published by the "Agenzia per l'Italia Digitale" (AgID).

Two main issues include:

a) Encryption of data: the use of encryption technology should not affect the availability of the data in case of any need to access them. It is therefore essential to ensure that, for the entire period of retention, the technology compatibility of the means, formats used to record the data, encryption equipment, and reading devices;
b) If cloud services are used, the service provider is mandated to expressly declare in the contract the exact location(s) of the data processed on behalf of the public administration.

Extended liability of legal entities for data protection crimes

The recent law decree n. 93/2013, dated 14 August 2013, which came into force on 27 August 2013, introduced an extended administrative liability of companies for criminal violations of the data protection law.

This decree amended and integrated the legislative decree no. 231 of 08 June 2001, "Provisions governing administrative liability of legal entities, companies and associations, including those lacking legal personality" ("Decree 231/2001"), which provides specific liabilities of the companies in relation to crimes committed by its top management and/or its staff when crimes are committed in the interest or in favour of the company. The related sanctions for the company can be of different kinds, including:

(i) Pecuniary sanctions. Sanctions ranging from a minimum of EUR 25,000 to a maximum of EUR 1,549,000;
(ii) Interdictory sanctions (e.g., *inter alia*, debarment from exercising activity, suspension or revocation of authorisations, licenses or functional concessions);
(iii) Confiscation;
(iv) Publication of the Decision.

Such liabilities can be avoided if the company proves that, before the crime or violation occurred, it had adopted and effectively implemented organisational and management models suitable for the prevention of the crimes listed in the Decree 231/2001.

The new law decree affects new crimes, such as computer fraud with substitution of the digital identity or falsification of credit cards, and crimes under the Italian Data Protection Code (such as the unlawful processing of personal data, untrue declarations and notifications to the Italian DPA and failure to comply with provisions issued by the Italian DPA).

These provisions are likely to have major repercussions as the violations potentially concern all entities involved.
Please note that this law decree has to be converted into law before 15 October 2013, and may therefore be subject to further changes.

Poland

New Soft Law on IT management and ICT security for the banking sector

Izabela Kowalczuk, Associate, and Mateusz Cina, Trainee, Bird & Bird (Warsaw)

A new Recommendation on IT management and ICT security in the banking sector ("**Recommendation D**") was issued by the Polish Financial Supervision Authority ("**KNF**") on 8th January 2013, which replaced the previous provisions from 2002. and has replaced the previous 2002 version. The KNF expects banks to implement the Recommendation by 31 December 2014.

Recommendation D is a soft law provision containing 193 recommendations divided into 22 categories. Most of the recommendations reflect global standards, such as those included in ISO/IEC 27001 on information security management.

Recommendation D lays out specific guidelines on data management, including data quality, cooperation between business areas and technical areas, system security, cloud computing, management reporting and other related issues. It also aims at raising awareness amongst bank employees and clients about the risks connected to IT systems used in banks by creating specific rules, education initiatives and a corporate culture.

We outline some noteworthy issues arising from Recommendation D:

Management & Data Security

Recommendation D contains many recommendations related to the general management and security of data. The KNF recommends that data should be categorised according to its character (e.g. importance). Each data category should have its own guidelines and an internal department responsible for maintaining them. Banks should also have written rules on data management regulating, *inter alia*, issues of data quality and confidentiality. Additionally, banks should consider establishing a committee responsible for data management.

Lack of Conformity with Personal Data Protection Law

Although Recommendation D specifically states that banks should follow rules set forth in the Personal Data Protection Act ("**PDPA**"), it seems that the KNF has not ensured that Recommendation D fully conforms with the PDPA. For example, the KNF recommends prohibition of data deletion from back-up copies. According to case law, banks are obliged to delete personal data from back-up copies when there are no legitimate grounds for storing them.

Some doubts concerning conformity with data protection law also arise regarding the background screening of employees. Under Recommendation D, banks should carefully select employees who will have access to confidential information. The question arises whether in order to fulfil the above obligation banks should check employees' criminal records, which as a general rule is forbidden, unless specific provisions allow employers to do so, e.g. members of the management board.

Biometrics

Aware of the huge potential in this area, the KNF recommends using biometrics combined with other authentication methods, e.g. passwords, to authenticate users and to control physical and digital access to systems and infrastructure when protecting critical data, functions and infrastructure. As Polish law does not allow employers unrestricted use of biometric methods to authenticate their employees, banks should confirm whether a particular biometrics solution is lawful. They should also check whether collecting biometric data is adequate and proportionate.

BYOD (Bring Your Own Device)

Recommendation D acknowledges this as an existing trend in the work place. If a bank allows its employees to use their own private devices for work purposes, it should firstly assess the risks associated with this and then implement appropriate internal rules. The bank has a broad discretion in formulating such rules. Recommendation D only states that such rules should specify:

- the permitted scope of use of private devices, indicating which data may be processed;
- the permitted devices;
- the software that employees may use for work purposes.

Banks should also ensure that these rules are fully adhered to and continuously monitored by specific software solutions. Employees should be trained on how to use their private devices for work purposes safely, and informed of the risks involved.

Sanctions

Although Recommendation D is a soft law provision, the KNF has the legal authority to force banks to implement it. The KNF is authorised by the Banking Law to issue recommendations directed to particular banks. The recommendation may pertain, *inter alia* to the risks connected with the banks' activities, which Recommendation D partially addresses. The KNF may find that a bank should reduce its risk by taking particular measures. These risks may be identified during the KNF's inspection on the implementation of Recommendation D. According to the Banking Law, if the bank does not follow the recommendation the KNF may exercise its statutory powers, including the power to impose fines or withdraw the banking license.

United Kingdom

Update: Guide to information requests under the Data Protection Act and recent case on subject access requests and retention of data

Laura Acreman, Associate, Bird & Bird (London)

Subject access code of practice

The Information Commissioner has published a subject access code of practice, which draws together existing guidance on dealing with subject access requests and provides additional advice and recommended best practice in this regard. The code of practice is aimed at all organisations that hold personal data, as they could be in receipt of an access request.

Bringing ICO guidance up to date, the code notes that the only requirement for an access request is that it is made in writing: email, fax, letter and even contact made via social media all satisfy this condition (although the means used for communicating a request may require greater or fewer checks on the identity of the requestor).

As a matter of good practice, the code encourages organisations to implement training and produce guidance for its staff so that they can recognise and appropriately deal with access requests.

• A reminder that data handled by your data processors is caught by the access requirements;

• The reasons for which an access request is made are irrelevant to your obligation to handle the request in accordance with the DPA;

• Archived records (including back-up copies where these are different to live data) are disclosable where they contain personal data; deleted records are not; and
• You may ask the requestor to narrow the scope of their request but they are entitled to ask for all of their personal data that you hold.
Bird & Bird's client briefing on handling access requests has been updated to incorporate this code and is available here

The full code can be found here.

In the matter of Southern Pacific Personal Loans Ltd & (1) Ian Christopher Oakley Smith (2) Julian Guy Parr (Applicants) & Information Commissioner (Interested Party) [2013] EWHC 2485 (Ch)

The High Court has issued a recent ruling examining the extent to which liquidators of a personal loans company would need to adhere to subject access requests made to that company. Since entering into liquidation in 2012, the company has been receiving approximately 88 subject access requests a month and the annual cost of handling such requests was estimated to be over £500,000. Most of the requests have been made by claims management companies seeking to determine whether individuals have a claim to compensation over the mis-selling of payment protection insurance.

This case determined that the liquidators would not be data controllers in respect of the data processed by the company prior to its liquidation and were therefore not personally liable for compliance with the Data Protection Act including responding to the subject access requests.

However, as agents for the company who would remain subject to the Act, they would still need to consider how such subject access requests would be handled.

Mr Justice David Richards held that given that the data in question was no longer required for any business of the company or for any purposes of the liquidation that it should be disposed of as soon as possible save that the company must retain sufficient data to enable it to:

(i) respond to any requests made to the company prior to the disposal date and

(ii) deal with any claims that may be made in liquidation.

The liquidators proposed to deal with the latter by advertising for claims against the company, inviting claimants to submit proofs and setting a date by which such proofs must be lodged. The judge helpfully confirmed that this was the right course of action and that "the liquidators are not under a duty to retain data so that it can remain available to be mined by former customers or claims handling companies with a view to making claims against third parties."

This case supports businesses who want to implement appropriate data retention/destruction policies and demonstrates how such policies can help to save them costs and protect against future claims.