December 2013

Data Privacy - A critical issue for business organisations

Data Protection has been gaining importance amongst the several fields of legislation that have an impact on the core activities of any kind of business and corporation. From the initial Council of Europe treaties, which began to establish criteria and guidelines for such regulation; through the EU Directive on Data Privacy, which has for many years set the legislative framework for Europe and for many other countries outside the EU also wanting to follow such a path; and now the imminent new European regulation, which will significantly increase obligations and procedures for all organisations.

The fact that the EU has decided to leverage the level of protection from a framework Directive to a unique Regulation for all member states, indicates how critical privacy is seen by regulators in the Union. It is clear that Europe, if it really wants to perform as a single and efficient market, cannot tolerate different legislative standards amongst the different member countries when it comes to determining how personal data must be treated. This is especially important for those categories of data treatments which, according to the current technological environment, will have a potentially sharp impact on individuals' privacy (such as behavioural monitoring), or potentially effect data subjects in several countries at the same time.

On top of the need to implement an effective harmonisation, EU regulators have also sent a clear message to agents in the market, so that privacy is fully understood to be a fundamental right whose protection and respect must at all times be considered by any organisation dealing with personal data. The result is that the new proposed EU Regulation seeks to introduce new protection principles, expressed in new accountability standards, the introduction of concepts such as "privacy by design", or the establishment of a very strong system of penalties.

These new protection principles will add new obligations, in addition to those already existing, which any organisation dealing with personal data will be forced to respect. Amongst these new obligations, the following are particularly worth highlighting:

- Introduction of new documentary and inventory obligations;
- Appointment of a Data Protection Officer within the organisation;
- Introduction of compulsory notification procedures to handle security violations affecting personal data;
- Compulsory risk assessments prior to the treatment of certain categories of sensitive data;
- Compulsory consultations and authorisations from data protection authorities prior to certain data treatments;
- A detailed regulation of erasure rights to ensure the effective enforcement of the "right to be forgotten";
- New procedures to ensure personal data portability; and
- Specific obligations on data profiling.

Consequently, future European regulation on personal data will imply more obligations and challenges to all organisations, located within the EU or outside its territorial scope.

In order to respond to such challenges, MERITAS has gathered a strong team of firms within the EMEA Region with the necessary capabilities, expertise and ability to provide the most comprehensive advice in this field - addressed towards the needs of businesses within the region, as well as those corporations with the aim of expanding or to establishing their businesses within the region - whose contact details can be found at the bottom of each of the country updates.

Carlos Pérez Sanz
Head of the Meritas EMEA Data Privacy Group

EU

Spanish and French Regulators fine Google for Data Privacy Violations

Ecija

The Spanish Data Protection Agency has imposed fines on the Internet giant Google Inc totalling €900,000 for what it considers "severe violations of the rights of citizens."

Grounds for the penalty start back in 2012, when Google merged its privacy policies intended to better align the services (nearly one-hundred) that it offers users. The Spanish Data Privacy Authority (AEPD) has since ruled that Google did not give users enough information about what personal data was collected and for what purpose it was to be used, that it unlawfully combines data obtained through all services, unduly stores data for an unlimited time and illegally rejects the rights of individuals to cancel and oppose the processing of their data.

Among the arguments put forward by the AEPD is that the combination of data collected via Google's different services greatly exceeds the reasonable expectations of most users, who are likely not aware of the process and thus lose control their own personal information.

To put things in context, the decision is the result of legislative initiatives impacting on Google and the result of joint action by EU Data Privacy Authorities gathered around the "Article 29 Working Group", which concluded that Google's new privacy policy was not compliant with the prevailing European data protection legislation. Accordingly, The Data Protection Authorities of Germany, Spain, France, Netherlands, Italy and United Kingdom have started similar enforcement actions, albeit Spain has had the "honour" of being the first to shoot.

France has however closely followed. Only weeks after the Spanish fine was announced, the French Data Authority (CNIL) imposed a fine of €150.000 on Google Inc, based on similar grounds, but with the additional obligation imposed on the internet giant to publish the decision on the google.fr website for at least 48 hours.

In addition to these penalties, future decisions might further compound Google's data privacy issues. Some months ago the EU Attorney General, Niilo Jääskinen, in a pre-judicial question submitted to the EU Court of Justice (ECJ) concerning the "right to be forgotten" confirmed that as Google performs the processing of personal data it must be subject to the EU Data Privacy Directive when it provides search

engine services in a Member State in order to promote and sell advertising space on its search engine - specifically considering the fact that Google has subsidiaries established in several members states each of which focuses the promotion of advertising activity towards the citizens of those states.

In conclusion, these decisions confirm the tendency for recognition of the application of data protection rules to service providers from outside the EU who have opened an establishment in the EU and who market advertising services in the EU. It is also not therefore strange that Google is now reportedly considering the establishment of data centres located in international waters; yes, in the open sea.

Carlos Pérez Sanz
Ecija
E cperez@ecija.com
T +34 933 808 255
www.ecija.com

Alejandro Touriño
Ecija
E atourino@ecija.com
T +34 917 816 160
www.ecija.com

Carlos Pérez Sanz is a Partner and Head of IT based in the Barcelona office of Ecija. He can be reached via cperez@ecija.com. Alejandro Touriño is a Partner and IT and Data expert located in the firm's Madrid office and can be reached via atourino@ecija.com.

BELGIUM

New protocol regulating international data transfer agreements

Lydian

On 25 June 2013, the Belgian Data Protection Authority (Privacy Commission) and the Ministry of Justice entered into a Protocol establishing new rules for the approval of international data transfer agreements outside of the EEA to countries that do not offer an adequate level of protection.

In the past, the authorisation for such international data transfers was only required when they were based on ad hoc data transfer agreements (i.e. non-standardised, tailor-made contractual clauses). If they were based on, and did not derogate from, one of the European Commission (EC) model contracts the controllers did not have to obtain authorisation from the Privacy Commission. However, according to this new Protocol, all contractual clauses used to transfer personal data outside the EEA must now be submitted to the Privacy Commission for prior approval.

Therefore, with respect to agreements based on the EC Model Clauses, before initiating their international data transfers the controllers subject to Belgian law will have to send their draft agreement (even if not amended) to the Privacy Commission, which will check its compliance with the EC Model Clauses. The controller will have to wait for formal written approval from the Privacy Commission, which will surely be granted when the draft international transfer agreement strictly incorporates the EC Model Clauses without any derogation and thus provides an adequate level of data protection.

On the other hand, with respect to ad hoc data transfer agreements, these previously needed to be approved by a Royal Decree (i.e. act signed by the King) after having obtained advice from the Privacy Commission and a review by the Belgian Council of State. The procedure was time-consuming and lacked clarity. A new simplified procedure has been adopted for the approval of such ad hoc data transfer agreements. The Privacy Commission now takes the lead in assessing whether the international data transfer agreement provides adequate safeguards (within 60 days from submission of the application). If the Privacy Commission determines that the guarantees are sufficient, the matter will be referred to the Ministry of Justice, which will approve the agreement by a Royal Decree based on a template attached to the protocol.

We regret that a formal approval is now required when using the EC Model Clauses. Broad international data transfer projects, notably involving other Member States, may therefore be delayed until the Privacy Commission grants such approval. Conversely, the simplified procedure for non-standardised agreements constitutes an improvement. It is one step forward and one step back. However, use of the EC Model Clauses is still likely to remain the faster and preferable solution to transfer personal data outside the EEA to countries that do not offer an adequate level of protection.

Annick Mottet Haugaard
Lydian
E annick.mottet@lydian.be
T +32 (0)2 787 90 13

Maroussia Verhulst
Lydian
E maroussia.verhulst@lydian.be
T +32 (0)2 787 90 00
www.lydian.be

Annick Mottet Haugaard is a Partner in the Brussels office of Lydian and Head of the Intellectual Property team. She can be reached via annick.mottet@lydian.be. Maroussia Verhulst is an Associate in the Brussels office and can be reached via maroussia.verhulst@lydian.be.

BULGARIA

What are the appropriate measures for protecting personal data?

Dimitrov, Petrov & Co.

Pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Directive), one of the main obligations of data controllers is to implement appropriate technical and organisational measures for the protection of personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves transmission of data over a network, and all other unlawful forms of processing.

The Directive does not however specify in detail what technical and organisational measures are appropriate and when the implemented measures will be considered appropriate. In this respect, data

controllers face difficulties assessing what is actually required to comply with this obligation and what the standards are for due care in this context. Ordinance No. 1 of 30th January 2013 (the Ordinance) adopted by the Bulgarian data protection authority - Personal Data Protection Commission (PDPC) - does nonetheless stipulate detailed requirements regarding the technical and organisational measures for the protection of personal data to be implemented by data controllers. The Ordinance is the most recent development in Bulgarian privacy and data protection legislation and is therefore significant from a practical point of view.

First, the new Ordinance abolishes previous rulings of the PDPC on the same matter, introducing significantly different concepts and requirements regarding the appropriate measures for the protection of personal data. This means that all Bulgarian data controllers are now obliged to thoroughly revise and change their internal data security policies. Second, the Ordinance introduces new formal requirements for data controllers to ensure written statements from company employees, and to prepare and keep up-to-date assessments on the level of impact of the personal data processed. Thus they must assess the personal data being processed and define the level of impact applicable to the respective data. Finally, the Ordinance specifies new minimum requirements regarding the different types of measures which should be implemented by controllers.

In the context of cross-border data transfers the new Ordinance may also have a significant impact on the international level. With a view to the requirement of data controllers to determine the applicable technical and organisational measures for protection in written contracts with their data processors and taking into account the provision of Art. 17(3) of the Directive, which stipulates that the applicable law regarding the technical and organisational measures for personal data protection shall be the national law of the Member State where the processor is established, foreign data controllers and processors (at the controller's instructions) should also or may need to comply with the new Ordinance.

Desislava Krusteva
Dimitrov, Petrov & Co.
E desislava.krusteva@dpc.bg
T +359 2 421 42 01
www.dpc.bg

Desislava Krusteva is a Senior Associate in the Sofia office of Dimitrov Petrov & Co. She can be reached via desislava.krusteva@dpc.bg.

FRANCE

Supreme Court voids the sale of customer lists for non-compliance with data protection law

Bignon Lebray

In a decision dated 25th June 2013, the Cour de Cassation, one of the Supreme Courts of France, voided the sale of a list of customers by a company as it had not been declared to the French Data Protection Authority (*Commission Nationale Informatique et Libertés* - CNIL).

In accordance with French data protection law, each data processing for a specific purpose (except for certain very limited exemptions) must be declared with the CNIL, one declaration being filed for each purpose.

A wine-dealer company in Bordeaux, in view of the retirement of its two partners, had sold for €46,000 its customer list (an Excel file including the name, address and phone numbers of its customers). The purchaser found that the customer list which was represented as including 6,000 customers only included 1,950 active customers and therefore tried to have the sale cancelled. The court of first instance and the Court of Appeals court both rejected this request but the Cour de Cassation overturned the decision of the Court of Appeals.

The purchaser pointed out that the customer file had not been declared to the CNIL, in breach of French data protection law. Since the file had not been subject to the formalities required by French data protection law, the *Cour de Cassation* found that it was illegal and therefore could not be sold. The solution would probably be the same for other breaches of French Data Protection law, such as failure to provide the data subjects with the compulsory information (purpose of the data processing, right to access and request modification of the data, identity of the data controller, etc) prior to the processing of their data.

This decision outlines the consequences of the failure to comply with data protection law in Europe. The most well known consequences of breaches of data protection law are the administrative and criminal sanctions which can be pronounced, as well as reputational damages. French law provides for strict administrative fines (up to €300,000) and for very high, although very seldom applied, criminal sanctions (fines up to €1,500,000 and up to 5 years of imprisonment).

The draft Data Protection Regulation that is currently being reviewed by the European Parliament provides for even higher administrative fines, of up 2% of the global turnover of the companies in breach of data protection law. However, in France civil sanctions are seldom applied, this decision being the first to our knowledge by a French court.

At a time where the data held by companies is becoming a key asset, compliance with data protection law is ever more important, since failure to comply can result in a severe loss of value of this intangible asset.

Marc Lemperière
Bignon Lebray
E mlemperiere@bignonlebray.com
T +33 (0)1 44 17 17 44
www.bignonlebray.com

Marc Lemperière is Of Counsel in the Paris office of Bignon Lebray. He can be reached via mlemperiere@bignonlebray.com.

GERMANY

Update on German Privacy Law: Fines, Employee Data, Court Ruling on Handling of Data by Irish Affiliate of US Company

SIBETH

Fines under the Data Protection Act 2009

Under Germany's Federal Data Protection Act (2009), the data protection authorities can impose fines of up to €300,000 for intentional or negligent breaches of privacy law, or even higher amounts as far as a company has gained financially from a breach. In 2010, several German banks were fined amounts in the lower six-figure Euro range for allowing freelance agents access to account activity data.

Draft Employee Privacy Act Has Failed

The Federal Government's proposal for an Employee Privacy Act was the subject of a controversial debate in Parliament in 2012 and 2013 and ultimately, the draft bill was withdrawn. As a result, the statutory rules in this area remain fragmented and are complemented by case law. The authorities frequently investigate complaints regarding the surveillance of employees and the handling of health-related data by employers. A health and beauty retailer was fined €137,500 in 2010 for the unlawful retention of employee health data and for not appointing a company data privacy officer.

Amendment of the Telecommunications Act

The Telecommunications Act was amended in 2012 to implement changes to the European Directive 2002/58 on privacy and electronic communication.

Court Rules on Processing of Personal Data of German Residents by Irish Affiliate of US Company

Companies from outside the European Economic Area (EEA) that collect personal data in Germany do not however have to comply with German Privacy Law provided that the data controller is "located" elsewhere in the EEA, e.g. Ireland or the UK. The requirements that have to be fulfilled by the company's establishment elsewhere in Europe in order to be exempt from German privacy law have been clarified as a result of a dispute between Facebook and a German supervisory authority.

Facebook Inc has an Irish affiliate which, according to the company, controls the handling of data by the social network Facebook in Europe. The Data Protection Authority of the tiny Federal state of Schleswig-Holstein argued, however, that German privacy law was applicable because Facebook also has a German affiliate. However, Facebook was able to convince the courts that the German affiliate is not involved in the handling of data of members of the social network.

The supervisory authority's second argument in favour of the application of German law was that Facebook's affiliate in Dublin does not "control" the German residents' personal data because the data being handled by the Dublin affiliate is actually stored on servers located in the US. According to the authority, Facebook therefore had to be treated as a company from outside the EEA transferring personal data to the US using equipment based in Germany (the users' personal computers). The court rejected this argument on the grounds that, according to the wording of the relevant provision of the European Directive, it is sufficient that the data processing is carried out "in the context of the activities" of an establishment of the controller on Irish territory (*Higher Administrative Court (OVG) Schleswig-Holstein, decisions dated 22 April 2013, 4 MB 10/13 and 4 MB 11/13*). Accordingly, the contractual and organisational rules regarding the responsibility for the handling of data within a group of companies are decisive and not the technical details. The supervisory authority has accepted the decision, calling on the European legislator to take steps against the persistence of "privacy law oases" in Europe.

Dr. Ulrike Elteste
SIBETH
E u.elteste@sibeth.com
T +49 (0)69 715 8996-0
www.sibeth.com

Ulrike Elteste is a Senior Associate in the Frankfurt office of SIBETH. She can be reached via u.elteste@sibeth.com.

GREECE

New data transfer obligations on credit institutions to tackle tax evasion

Tsibanoulis & Partners

Article 82 section 2 of the Greek Income Tax Code was amended by Article 8 section 7 of the new Tax Law 4110/2013, passed on January 11th 2013. This creates an obligation by tax-payers, public services, legal entities and organisations in general to submit electronically to the Ministry of Economy and Finance upon relevant request any data and information of financial and tax significance including the financial status of taxation subjects.

This amendment constituted the legal grounds for the recent issuance of Circular No. 1191/2013 (Circular) of the Minister of Economy and Finance, published in Government Gazette Issue B' No. 1926/8.8.2013, as regards the relevant obligation of credit institutions. In particular, the Circular provides for the details of direct internet transmission through a secure transfer system to the Ministry's General Secretariat for Information Systems (GSIS) of collected data relating to customers of credit institutions indicating an increased risk of tax evasion, this includes:

- Self-employed individuals holding or being the actual beneficiaries of bank accounts credited with more than €200,000 during the preceding calendar year; and
- Legal persons whose bank accounts were credited or debited with more than €300,000 in total during the preceding calendar year.

The transmissions must include the following data:

1. Tax Registration Number and competent Tax Office
2. *Individuals*: full name, date of birth, nationality, professional activity, address, telephone number, identity document number (ID/Passport). Legal persons: company form, name, seat, legal representatives (full name, tax registration number);
3. Details of all bank accounts held by the customer at the credit institution or to which the customer is a co-beneficiary;
4. Full name and Tax Registration Number of any co-beneficiaries to the bank accounts under 3 above;
5. Total balance of all the customer's bank accounts as of January 1st and December 31st of each year;

6. Total amount credited each year to all the customer's bank accounts (including transfers from other banks and cash or cheques, but excluding renewals of time deposits as well as transfers between different bank accounts of a customer held with the credit institution); and
7. *Legal persons*: total cash deposits and withdrawals realised each year with regard to all the customers' bank accounts (excluding deposits and withdrawals between different bank accounts held at the same credit institution)

The data may be transferred annually until April 30th of the year following the reference year. Credit institutions are obliged to store the transferred data for at least three months after transmission while the GSIS may store the date for up to 6 months after receipt. The infringement of said obligations may result in administrative fines ranging between €5,000-€100,000.

The Circular applies to data concerning the financial year 2011 and onward. The first data transfers concerning 2011 had to be realised by 30th October 2013, while data for 2012 may be transferred until 31st December 2013. Data processing for the above purposes requires neither prior notification/ consent of the data subjects nor the Data Protection Authority.

Dr. Christina Koutsogianni-Hanke
Tsibanoulis & Partners
E c.koutsogianni@tsibanoulis.gr
T +30 21 036 75 100
www.tsibanoulis.gr

Dr. Christina Koutsogianni-Hanke is a Senior Associate in the Athens office of Tsibanoulis & Partners. She can be reached via c.koutsogianni@tsibanoulis.gr.

IRELAND

Update on Privacy Law in Ireland

Whitney Moore

Data Protection Commissioners 2012 Annual Report

The Irish Data Protection Commissioner (DPC), Billy Hawkes, published his Annual report in May 2013 which emphasised the increasing significance of data protection law. The report highlighted the issue of sharing personal data in the public sector and whilst noting the benefits involved, he nonetheless advised that the sharing of data must be done in a way that respects the rights of the individuals in question. The necessity to ensure that personal data was not accessed or used without justification was specifically mentioned.

In 2012 1,349 complaints were received by the DPC, the majority of which related to compliance with data access requests and breaches of direct marketing rules. It also reported that 40 scheduled audits were carried out to monitor compliance with Data Protection Acts 1998 and 2003. The findings of these audits noted a reasonably high awareness of and compliance in Ireland with data protection principles in the inspected organisations.

The DPC also participated in a Global Privacy Enforcement Network (GPEN) internet privacy sweep in September 2013 along with various other privacy enforcement authorities. This involved a trawling by

participating authorities of 79 websites with a view to evaluating the privacy practices of organisations as outlined in the privacy policies on their websites or within their mobile applications. The DPC stated that the results of the sweep were encouraging in that 48 websites scored a score of 5 or more, whilst 14 achieved the top score of 6.

Memorandum of Understanding between the DPC and the US Federal Trade Commission
In June 2013, a Memorandum of Understanding (MOU) was entered into between the DPC and the chief US consumer privacy agency, the US Federal Trade Commission (FTC). The aim of the MOU is to support increased cooperation and communication between the two agencies in their efforts to ensure protection of consumer privacy and data protection rights. Although it is not legally binding, both countries commit to using 'best efforts' to share information and provide assistance where certain privacy violations are identified. This is an important cross-border development as many US multinational companies have subsidiaries or headquarters based in Ireland.

Recent Case law in Ireland
The case of *Collins v FBD Insurance plc [2013] IEHC 137* dealt with the extent to which a data subject may be entitled to damages for a breach of their data protection rights under the Data Protection Acts 1988 and 2003 by a data controller or a data processor. The defendant had, amongst other things, failed to supply personal data requested by the plaintiff within the prescribed forty day time limit. It was held that the legislation does not go beyond the obligation for compensation contained in the Data Protection Directive 95/46/EC, which does not provide for either strict liability or the automatic payment of compensation and instead provides for the existence of a duty of care. Although breaches of data protection rights had occurred, it was held by the High Court that a right to compensation does not automatically flow from such a breach unless loss or damage can be proven and the earlier award by a Circuit Court of €15,000 was overturned.

EU Regulation 611/2013
The new EU rules on the notification of personal data breaches by telecommunications operators and internet service providers came into force in Ireland on 25th August 2013 when the Regulations became directly applicable in Ireland.

Emma Richmond
Whitney Moore
E emma.richmond@whitneymoore.ie
T +353 1 611 0000
www.whitneymoore.ie

Emma Richmond is an Associate in the Dublin office of WhitneyMoore. She can be reached via emma.richmond@whitneymoore.ie.

ITALY

Italy's new "*marketing and anti-spam*" guidelines

Pirola Pennuto Zei & Associati

The Italian Data Protection Authority (*Garante per la protezione dei dati personali - GPDP*) has issued new *Marketing and anti-Spam Guidelines* to counter wildcat marketing and to promote consumer-friendly commercial practices (published in the Italian Official Gazette NO. 174 of 26th July 2013).

In particular, the GPDP has decided to define a first consolidated set of measures and precautions that can be helpful both to companies planning marketing campaigns to advertise their products or services, and to any individual wishing to fend off intrusions by companies using their personal contact information without asking for prior consent.

In defining such Guidelines, the GPDP - on the one hand - has identified conducts that are certainly illegal and - on the other hand - has determined the main rules that shall be followed in order to treat consumers' personal information legally.

In light of the above, the GPDP has defined as illegal cases in which a social network user receives, in private or on their personal "wall", promotional messages for a specific product or service from a company that has drawn the data recipient's personal profile from the social network to which the user is registered, unless the company documents a specific consent in this respect.

In relation to legal treatments, the GPDP has defined that companies shall respect principles of "necessity" and "proportionality", defined respectively in Articles 3 and 11 of Legislative Decree No. 196/2003 (Italian Privacy Code), when processing personal data.

In fact, according to Article 3, information systems and computer programs shall be configured by minimising the use of personal data and identification data. On the other hand, Article 11 establishes that personal data processing must be:

- processed lawfully and fairly;
- collected and recorded for specific, explicit and legitimate purposes and used in operations compatible with the above purposes;
- accurate and, where necessary, updated;
- adequate, relevant and not excessive in relation to the purposes for which they were collected or subsequently processed; and
- kept in a form which permits identification of data for a period of time no longer than necessary for the purposes for which they were collected or subsequently processed.

According to such principles, the GPDP has summed up the rules on the most common new frontiers of marketing, such as "social spam" (performed on the internet or via social networks) and "viral marketing" (promotional activity lead through the communicative ability of a few individuals who are able to convey marketing messages to a large number of final consumers).

The goal of the GPDP is to encourage the protection of consumers' privacy - who are often not aware of the treatment that their personal data undergoes - with the necessity for companies to reach consumers with new information methods, thus keeping businesses in step with the development of new technologies and social networks.

We are available to provide full details on this new provision, as well as to update on future development of the same legislation.

Mario Valentini
Pirola Pennuto Zei & Associati
E mario.valentini@studiopirola.com
T +39 6 570 281
www.pirolapennutozei.it

Mario Valentini is a Partner at Pirola Pennuto Zei & Associati in Rome. He can be reached via mario.valentini@studiopirola.com.

LUXEMBOURG

New rules surrounding the notification of personal data breaches

LG@vocats

Currently in Luxembourg there exists an obligation on electronic communications service providers only to notify the authorities of a personal data breach; albeit a proposal is pending to introduce a wider general notification obligation.

This, more narrow, obligation was introduced by Directive 2009/136/EC dated 25th November 2009 (modifying Directive 2002/58/EC) and implemented in Luxembourg by the Law of 28th July 2011.

Under Directive 2009/136/EC (and the Law of 28th July 2011), "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Community.

In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the Luxembourg Data Protection Authority (*La Commission Nationale pour la Protection des Données - CNPD*).

The new Regulation 611/2013 dated 24th June 2013 and which entered into force on 25th August 2013 in all EU Member States, provides specific measures applicable to the notification of personal data breaches.

In particular, the provider shall notify the breach to the competent data protection authority no later than 24 hours after detection, where feasible.

The provider must however include in its notification to the competent national authority very precise information. This information includes the date and time of the incident, the circumstances of the personal data breach (e.g. loss, theft, copying), the nature and content of the personal data concerned, any technical and organisational measures applied (or to be applied) by the provider to the affected personal data, a summary of the incident that caused the data breach (including the physical location of

the breach and the storage media involved), as well as the number of subscribers or individuals concerned.

Furthermore, it is to be noted that the data protection authority has to provide to all providers established in the Member State concerned a secure electronic means for notification of personal data breaches and information on the procedures for its access and use.

In Luxembourg, a form is available on the website of the CNPD which has to be used by electronic communication service providers in cases of a personal data breach. However, this form should be amended in order to include the information requested under the new EU Regulation.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach. The CNPD is allowed, in cases of repeat violations of the obligation to notify it of a personal data breach, to deliver fines up to €50,000. Such a sanction is however, in practice, rarely applied.

Hervé Wolff
LG@vocats
E hw@vocats.com
T +352 443 7371
www.vocats.com

Hervé Wolff is a Partner at LG@vocats in Luxembourg. He can be reached via hw@vocats.com.

POLAND

Personal data protection in Poland

Domański Zakrzewski Palinka

Personal data protection is regulated comprehensively in Poland by the Personal Data Protection Act of 29th August 1997. It elaborates on the general regulation of Article 51 of the Polish Constitution, which affords legal protection to personal data.

This Polish Act is largely identical to Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It also reflects international regulations on personal data protection, especially the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28th January 1981 (Convention No. 108).

While Polish laws implement EU regulations, certain unique rules exist as regards the application of the law in practice. For instance, in Poland (unlike some other European jurisdictions), Model Contractual Clauses and Binding Company Rules are not independent legal bases for data transfers to third countries. Data can only be transferred subject to the prior consent of the Polish Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych - GIODO). This is very important in practice.

The GIODO believes that the main rules and the constitutional data privacy protection scheme have been proven to work in practice but some Polish regulations on personal data protection are obsolete and should be changed. This is due especially to technological progress, including the development of the internet.

In the context of the impact of technology changes on data protection, smart metering and cloud computing has recently been discussed extensively in Poland. Our law firm is involved in both of these issues, advising clients on specific matters and preparing reports to promote wider knowledge of this area. It is worth noting that the need for a global change to personal data protection law was discussed during the 35th International Conference of Data Protection and Privacy Commissioners, held in September 2013 in Warsaw.

Apart from proposing legislative changes due to technological progress, for some time now, the GIODO has also been seeking the right to impose financial penalties on parties for breaches of personal data protection regulations. This right would strengthen the GIODO's position and could lead to increased compliance with data protection laws. On the other hand, it could result in a more rigorous law application system.

Bartosz Marcinkowski
Domański Zakrzewski Palinka
E bartosz.marcinkowski@dzp.pl
T +48 22 557 76 17

Rafał Surowiec
E rafal.surowiec@dzp.pl
T +48 61 642 49 60
www.dzp.pl

Bartosz Marcinkowski is a Partner at Domański Zakrzewski Palinka in Warsaw. He can be reached via bartosz.marcinkowski@dzp.pl; Rafał Surowiec is an Associate in the Warsaw office and can be reached via rafal.surowiec@dzp.pl.

ROMANIA

Romanian Data Authority clarifies rules on use of video surveillance

Banu Raclaru & Nasta

Romania, as a European Union (EU) member state, has aligned its domestic legislation with EU law, including regarding the protection of personal data.

The domestic legislation in this respect is Decree Law No. 677/2001 on the *Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data*, with subsequent amendments.

Based on this framework law and paragraph 14 of Directive 95/46/EC of the European Parliament, the relevant Supervisory Authority in Romania, the National Authority for Surveillance and Personal Data

Processing (*Autoritatea Nationala privind Supravegherea Prelucrarii Datelor cu Caracter Personal - ANSPDCP*) has issued a number of guidance decisions.

Among the most recent decisions issued relates to the processing of personal data by use of video surveillance (Decision No. 52/2012). Among other things, this decision clarifies that an entity may not allow the processing of personal data of employees by means of video surveillance inside the workplace, unless expressly stipulated by law (for example, when employees have expressly given their consent prior to processing), or with the opinion of the ANSPDCP.

In applying these legal rules, the Authority recently rejected the request of local authorities to receive notice by employees through video surveillance in their offices, considering that any use of cameras is allowed only with the unambiguous consent of the person concerned or, exceptionally, under the conditions stipulated by the law limiting when such consent is required with respect to the principle of proportionality, processing purpose and based on the prior information of the individuals concerned.

According to the order, the duration of data storage obtained through video surveillance should be proportional to the purpose for which the data is processed, but not more than 30 days, unless expressly stipulated by the law or where duly justified. After this period the data must be erased or destroyed depending on the medium in which it was stored.

Oana Elena Nasta
Banu Raclaru & Nasta
E oana.nasta@brnlegal.ro
T +40 21 210 65 55
www.brnlegal.ro

Oana Elena Nasta is a Partner in the Bucharest office of Banu Raclaru & Nasta. She can be reached via oana.nasta@brnlegal.ro.

SPAIN

New Spanish guidance on the use of Cookies

Ecija

As result of recent changes in the regulation of commercial electronic communications and the related use of personal data for such purposes through the use of Cookies, the Spanish Data Protection Agency (*Agencia Española de Protección de Datos - AEPD*), which has the power to impose fines as result of breaches of Spain's anti-spam legislation, has recently published a new *Guide on the Use of Cookies*.

Following recommendations issued by the Article 29 Group of the European Union (EU), the Guide includes legal advice and recommendations encompassing the following subjects:

a. Technical guidance on the legal implications and technical issues related to the use of cookies (types of cookies by purpose, term or data controller, legal definitions of equipment, website, promotional space, etc);
b. Indications on which cookies are subject to prior data subject consent, and which cookies are exempted from such consent;

c. Responsibilities of the agents involved (editors, publishers, promotional networks, advertisers and companies providing statistical services, etc); and
d. Guidance on how to provide proper information to data subjects and the correct way to obtain online consent for the use of data in connection with cookies.

The full text of the Guide on the Use of Cookies issued by the AEPD can be found at www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf. Since this text is however in Spanish, we can on request provide detailed explanations and advice about the implementation of website privacy policies, the use of cookies and related processing of personal data of website visitors and users.

Carlos Pérez Sanz
Ecija
E cperez@ecija.com
T +34 933 808 255
www.ecija.com

Carlos Pérez Sanz is a Partner and Head of IT based in the Barcelona office of Ecija. He can be reached via cperez@ecija.com.

SWITZERLAND

Swiss Data Commissioner's FATCA data transfer principles

Wenger & Vieli

In 2013, the Swiss Parliament had to deal with the issue of the cross-border transfer of private data in connection with US authorities' demands for the disclosure of personal data of employees and third parties from Swiss banks in connection with suspected cases of tax evasion. The Swiss Federal Council proposed a new act named "Lex USA" that would have enabled banks to disclose information on accounts held by US citizens, as well as on bank employees and others who assist them, to the US authorities. The Swiss Parliament, however, rejected the proposal.

A Geneva court had to rule on a case where a bank claimed an overriding public interest to justify the cross-border transfer of the employee's data with. The court acknowledged that the stability of Switzerland as a financial centre could qualify as an overriding public interest. At the same time it ruled that the interests of the concerned employee must be weighed against those of the public in each individual case. In the case presented, the bank made only general statements about the necessity of the data transfers to the foreign authorities. The employee, however, gave a fair representation of the threat of prosecution by the foreign authorities. This prompted the court to prohibit the data transfer.

As regards cross-border data transfer, the Swiss Federal Data Protection and Information Commissioner (FDPIC) issued a factsheet for banks on the transmission of personal data to the US authorities (dated 20th June 2013, based on recommendations issued by the FDPIC on 15th October 2012). To comply with these regulations, the transfer of personal data relating to employees and third parties must adhere to the following principles:

1. *Proportionality principle* (Art. 4 para 2 Data Protection Act - DPA): Data may only be processed (which includes data transfer) if needed for a specific purpose;
2. *Transparency principle* (Art. 4 para 2 and 4 DPA): The bank must notify the persons and legal entities concerned of the extent and nature of the documents that are to be transmitted including information as to the period to which they relate to;
3. *Right to information* (Art. 8 DPA): The bank must allow those concerned a suitable period in which to be given information on all the documents relating to them;
4. *Justification* (Art. 6 and 13 DPA): If a person or legal entity objects to the bank transmitting documents containing their data, the bank must weigh up the interests in that specific case. The bank must both claim justification for the transmission and fulfil the requirements of Art. 6 DPA before data may be transmitted to a country that does not have legislation that guarantees adequate data protection. In such cases, sufficient guarantees for an adequate data protection must be obtained; and
5. *Legal claims* (Art. 15 DPA): If the bank intends to transmit the data against the will of the person concerned; the bank's decision may be challenged in the civil courts.

The FDPIC asked all banks wishing to transmit personal data to agree to comply with the procedures set out in the recommendations and factsheet and to notify him of any planned transmissions of data. In the meantime, lawmakers are examining alternative ways to ease the cross-border disclosure of data in connection with the implementation of the US Foreign Account Tax Compliance Act (FATCA), which requires banks to report funds held by American citizens.

In addition, the US Department of Justice (DoJ) has introduced a program for Swiss banks (announced August 29th 2013) enabling them to resolve their criminal and civil exposure with the DOJ's Tax Division in connection with cases of suspected tax fraud. Participation in the program would require the disclosure of personal data of the various persons involved (employees, trustees, etc). It remains to be seen which banks will join the DOJ's program and also how the Swiss courts will judge such cross border transfers of personal data.

Claudia Keller
Wenger & Vieli
E c.keller@wengervieli.ch
T +41 (58) 958 58 58
www.wengervieli.ch

Claudia Keller is a Senior Associate in the Zurich office of Wenger & Vieli. She can be reached via c.keller@wengervieli.ch.

UNITED KINGDOM

UK regulator warns law firms on the use of cloud services

HowardKennedyFsi LLP

The Solicitors Regulation Authority (SRA) is the regulatory body of the Law Society of England and Wales. In November 2013, the SRA published guidelines for law firms on the use of cloud computing services, focusing on the data protection challenges inherent in the new technology. The SRA guidelines will therefore be of interest to law firms wherever they may be in Europe.

The SRA points out that as lawyers, we have a special duty to our clients to keep client information strictly confidential. We must therefore ensure that we do not chose providers which might compromise that confidentiality. In the virtual environment, your client data could be stored on the same servers as data belonging to many others, with no physical separation and only a password and log-in preventing authorised access.

The UK's Data Protection Act 1998 sets out 8 key "Principles" of data protection, drawn from the 1995 European Directive. The 7th Principle of Data Protection is that personal data must be kept securely. It is therefore incumbent on the law firm as "Data Controller" to ensure that the cloud provider has adequate security measures in place. We are not of course expected to be data security experts, but checking to see if the provider's security has been independently audited is easy to do. Is it, for instance, compliant with internationally recognised standards, such as ISO/IEC 27001:2005?

The SRA also suggests that the law firm itself can play a part in boosting the security by encrypting the data within the law firm before it is transmitted to the cloud provider.

The 8th Data Protection Principle is also highly relevant. This Principle prohibits the transfer of personal data outside the EEA without "adequate protection". This is very much an issue when the cloud provider (or its servers) is based outside the EEA, particularly if it is a US company, since the laws of the USA are deemed by the EU not to provide "adequate protection" for personal data.

If choosing a US based provider, the law firm should check if that provider has registered for the US Safe Harbor Scheme. That may provide some comfort but even then, there are risks. US companies are subject to strong data seizure legislation (under the US PATRIOT Act) and, it would appear from recent revelations in the press, extensive surveillance by the National Security Agency (NSA). The SRA points out that it now appears that the US Government has the power to easily harvest metadata - information such as recipients and subject lines of emails. That is enough to reveal networks of individuals and could lead to a breach of confidence by the law firm, by revealing, for example, when a firm is involved in confidential merger discussions. The SRA therefore warns that law firms should give "serious consideration" to the risks of storing data in the USA.

Cloud computing brings with it many risks. Aside from the legal risks, there are also commercial risks, such as the risk of the provider's downtime bringing the business of the law firm to a standstill.

However, the SRA is not blind to the benefits of cloud computing, not least the cost advantages and flexibility of the solutions offered. Further, it points out that in some cases, the security features and encryption offered by some cloud providers may actually be better than could be achieved by a small law firm storing its data locally. To quote a peculiar British idiom, "every cloud has a silver lining".

The SRA guidelines, entitled "Silver Linings: Cloud Computing, Law Firms and Risk" can be found at www.sra.org.uk/riskresources.

Robert Lands, HowardKennedyFsi LLP
London
2nd December 2013

Robert Lands

HowardKennedyFsi LLP
E robert.lands@hkfsi.com
T +44 (0)20 3350 3350
www.howardkennedyfsi.com

Robert Lands is a Partner and Head of IP and IT at HowardKennedyFsi in London. He can be reached via robert.lands@hkfsi.com.

USA

Lack of injury means lack of standing to sue in US data breach claims

Stradley Ronon Stevens & Young

Two recent Federal Court decisions follow a growing line of Federal and State decisions dismissing tort and other claims in data breach cases on various grounds, including the notable challenge plaintiffs face in making out the element of injury to satisfy their pleaded claims. Most recently, on September 3rd 2013, the US District Court for the Northern District of Illinois dismissed a class action against Barnes & Noble stemming from a credit card "skimming" incident that occurred in 2012 (*Barnes & Noble Pin Pad Litigation, No. 12-cv-8617 - N.D. Ill*). The Court held that the plaintiffs failed to satisfy the elements of Article III (standing) and dismissed all five pleaded causes of action. The Barnes & Noble Pin Pad decision highlights the ongoing challenges faced by plaintiffs in data breach litigation to articulate injury both for the purposes of Article III and in order to state a claim for relief.

In disposing of most of the claims asserted against Barnes & Noble, the District Court relied on the Supreme Court's 2013 decision in *Clapper v. Amnesty Int'l (USA, 122 S.Ct. 1138 - 2013)*, wherein the Court explained that an injury that is "certainly impending" can, in fact, be considered an injury for the purposes of standing, though "[a]llegations of possible future injury are not sufficient." Thus, the allegation of mere increased risk of identity theft or fraud, even though couched as "substantial" in the complaint, did not meet the Clapper standing requirement of certain impending harm. Likewise, the Court viewed the statutory claims to be deficient because plaintiffs merely pleaded violations of the statutes, but no injury. Moreover, the statutes themselves plainly state that the customer must suffer damages or injury.

In the other recent case involving data breach claims, *Benjamin Bell, et al. v. Blizzard Entertainment, Inc. (No. 12-CV-09475-BRO - C.D. Cal, July 11, 2013)*, the US District Court for the Central District of California granted the defendant's motion for judgment on the pleadings dismissing most of the claims brought against Blizzard Entertainment, Inc. refusing to allow common law claims to be asserted against Blizzard following a data breach the company incurred in 2012. This decision is another good example of the ongoing obstacles plaintiffs face in asserting such common law claims against entities that experience data security breaches. Lack of proof of damages remains the principal obstacle to such claims, although there were additional grounds for dismissal of the claims in this case also.

Nicholas Deenis
Stradley Ronon Stevens & Young
E ndeenis@stradley.com
T +1 484 323 1351
www.stradley.com

Nicholas Deenis is a partner in the Malvern, Pennsylvania, office of Stradley Ronon Stevens & Young. He can be reached at ndeenis@stradley.com.