DechertOnPoint

April 2007 / Issue 2

A legal update from Dechert's Data Protection and Privacy Group

Data Protection Developments in Europe, from Whistleblowing Principles to Security Breach Planning

In this issue of our regular data protection and privacy updates we highlight some recent developments in individual member states around Europe.

In Belgium, the SWIFT saga continues with the Belgian Privacy Commission issuing a strong second advisory opinion on SWIFT's failure to comply with its obligations when transferring data to the US. The Commission also issued a recommendation containing basic principles on whistleblowing, which will affect companies which implement whistleblowing schemes.

In Germany, the thresholds for the requirement for a data protection officer have been increased. In France, the regulator (CNIL) has sought to balance the prohibition on collecting data relating to a person's racial or ethnic origin with employers' needs to collect such data in order to implement policies preventing racial and ethnic discrimination in the workplace.

Whilst in the UK, security breaches are all the rage, with the FSA applying a fine of almost £1 million on Nationwide Building Society, and the Information Commissioner accepting undertakings from other banks for their disposal of personal data. These serve as a reminder that firms must continue to assess Information Security risks, and to evolve plans for dealing with breaches of security.

Belgium

SWIFT

The SWIFT saga continues. By way of background, the operations centres of SWIFT, the worldwide financial telecommunications network operator, in Belgium and the US each hold all messages processed by SWIFT, which includes information about transactions occurring entirely outside Europe. The US Treasury Department had served subpoenas on SWIFT requesting general data (the requests were not specific to particular individuals or dates). SWIFT had not informed any EU authorities, Member States or clients of this, but elected to enter into secret negotiations with the Treasury Department regarding the data it would hand over. The Belgian Privacy Commission held SWIFT to be in breach of its obligations as a data controller, specifically failing to inform regulatory authorities of its processing, and failing to comply with the rules concerning personal data transfer to countries outside the EEA.

To bring the matter up to date, following the request of the Belgian Prime Minister, the Belgian Privacy Commission in December analysed the SWIFT case in greater detail and issued a second advisory opinion, which confirmed and built further on both an earlier such opinion as well as the November 2006 opinion of the European Article 29 Working Party.

Although recognizing the existence of a situation of conflict between American and European law, and the fact that SWIFT made considerable efforts to provide certain guarantees through its negotiations with the United States Treasury Department, the Privacy Commission confirmed that SWIFT should have, but failed to, comply with several obligations contained in the Belgian Privacy legislation (i.e. the notification obligation and the obligation to comply with the rules concerning personal data transfers to countries outside the EU).

Whistleblowing Hotlines

The Belgian Privacy Commission recently issued a recommendation with respect to the compatibility of whistleblowing schemes with the Belgian Private Data Protection Law of 8 December 1992.

In this recommendation, the Belgian Privacy Commission indicated that since the Private Data Protection Law applies as soon as personal data is processed by automatic means or is filed or is intended to be filed, it will apply to almost all whistleblowing schemes. The Commission outlined a number of basic principles, which should at least be respected by whistleblowing schemes to be compatible with the Private Data Protection law. These principles are more detailed than the earlier recommendations of the Article 29 Working Party (see our update of August 2006 at http://www.dechert.com/library/DP_Issue1_08-06.pdf) and relate to (i) honesty, legitimacy, purposefulness of the scheme, (ii) proportionality, (iii) accuracy of the personal data, (iv) transparency, (v) security of the processing operations and filing, (vi) rights of all persons involved (whistleblower, reported person and third parties), and (vii) registration of the database if the data will be automatically processed or at the request of the Belgian Privacy Commission.

The recommendations of the Belgian Privacy Commission are not binding but have an important persuasive authority, and are normally followed by the courts. Therefore, their practical impact is significant and the basic principles can be used as a guideline for companies wishing to implement whistleblowing schemes in Belgium.

France

Collection of Data to Measure Diversity of Employees in France

The French data protection law of 1978 (Article 8) as a general principle prohibits the collection and processing in France of personal data which directly or indirectly shows a person's racial or ethnic origin, except in certain limited cases. However, the fight against discrimination, in particular against racial or ethnic discrimination in the workplace[1], which has become a public priority[2], has led employers in France to implement tools to measure the diversity of the origin of its employees, and thereby collect and process personal data which could show a person's racial or ethnic origin.

As a result, the French Data Protection Authority (so-called CNIL) "*Commission Nationale Informatique et Libertés*" issued recommendations on the methods to be used in order to measure the diversity of the origin of employees. Prior to implementing such diversity policies, employers must discuss their objectives with the personnel representatives. Only the use of data which is pertinent vis-à-vis the objectives of the study on diversity within the company and/or company anti-discrimination policy may be used. Certain personal data such as the candidate's or employee's first name, last name, current and original nationality, place of birth, address and parents' nationality or birth place may be collected and processed in order to implement tools to measure the diversity of origins, but the CNIL recommends that data relating to the employee or candidate's original nationality or the nationality or place of birth of his/her parents not be saved in the HR files given the sensitivity of such data and its uncertain relevance. The collection of such data would only require the filing of a normal declaration with the CNIL (as opposed to an authorization). Other data, especially data related to racial, real or presumed ethnic origin, should in no event be collected by employers as there exists no national or regional ethnic-racial statistics in France with which to compare, as there does in the United States. In any event, concerned employees must be informed of the processing on such data, its objectives, the recipients of such data, their rights of opposition, access and rectification. Such processing must be carried out confidentially and must guaranty the anonymity of the employees concerned. After statistics have been issued, the CNIL recommends that the individual data files be destroyed.

Germany

In August 2006, the so called Act on Reduction of Bureaucratic Obstacles, in particular for medium-sized businesses (*Erstes Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft*) was enacted. This act

[1] Pursuant to Article L.122-45 of the French Labor Code, no person may be excluded from a recruitment procedure, no employee may be sanctioned, dismissed or subject to a discriminatory measure owing in particular to his/her origin, his/her actual or presumed belonging to an ethnic group, nation or race. Despite these provisions, case law on racial discrimination is relatively scarce in France.

[2] A High Authority to Fight against Discrimination and for Equality (the so-called HALDE) was created in 2005.

amended the provisions of the German Data Protection Act (*Bundesdatenschutzgesetz*) dealing with the threshold for the appointment of a Data Protection Officer (*Datenschutzbeauftragter*) in a company. If a certain number of people are concerned with personal data in the company, such an officer must be appointed. The officer is obliged to ensure that the company complies with the applicable data protection laws. The threshold for people concerned with automatic data processing (*automatische Datenverarbeitung*) of personal data has now increased from five to ten people. The threshold for those concerned with manual data processing (*manuelle Datenverarbeitung*) of personal data has not changed and remains twenty. Accordingly, a company is obliged to appoint a data protection officer, if either of those thresholds have been reached.

For companies which have already appointed a data protection officer according to the former laws, such data protection officer can be revoked if a company has less than ten people concerned with automatic data processing. However, it should be noted that a company has to assure that it is in compliance with the applicable data protection laws at all times, i.e. regardless of the obligation to appoint a data protection officer.

United Kingdom

FSA takes action over security breaches by Nationwide

Nationwide Building Society found itself the subject of a great deal of unwanted publicity last November when it emerged that a laptop stolen from the home of an employee in August 2006 contained customer information. On 14 February 2007 this security lapse resulted in the UK Financial Services Authority fining Nationwide £980,000. The fine would have been £1.4 million but for Nationwide's cooperation with the investigation and agreement to settle at an early stage.

The FSA found that Nationwide's security systems and controls were inadequate and, as such, Nationwide had breached Principle 3 of the FSA's Principles for Business: "*A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.*" The FSA criticised Nationwide's assessment of risk regarding the security of its customer information, and Nationwide's procedures and controls in managing those risks. Nationwide had failed adequately to train and monitor staff, and to have appropriate management procedures to deal with a breach of security. Nationwide's investigations of what information the laptop contained were inadequate (it was a full three weeks after the theft was reported that it realised that the laptop contained customer information) and inhibited its ability to respond rapidly. As such, although no financial crime had been committed here, there had been an increased opportunity that the information could have been used for such purposes. In November 2004 the FSA published a report entitled "*Countering Financial Crime Risks in Information Security*", and believed that as a result of this report (and other related activities) there should have been an increased awareness of the risks of identify theft. The FSA found it was particularly serious that Nationwide's security measures had not been enhanced as a result of this heightened awareness despite internal recommendations of its own staff.

This is a salutary reminder of the need for proper security to be put in place by those controlling customer data.

ICO also takes action over security breaches

On 12 March 2007 the Information Commissioner's Office (ICO) found eleven banks to be in breach of their obligations as data controllers under the Data Protection Act 1998. The ICO received and investigated complaints regarding the processing of personal data at certain branches of various institutions including The Royal Bank of Scotland, National Westminster Bank plc, Barclays Bank plc, The Co-operative Bank plc and, again, Nationwide. Each was found to have disposed of documents containing personal data of its customers in waste receptacles outside branch offices. Items which were found include standing order details, customers' names and account numbers, details of a PIN number to a customer's account, completed insurance application forms, and personal financial overviews for customers.

As a result of the findings of the ICO investigation, the banks signed formal undertakings to comply with the data protection principles. Deputy Commissioner David Smith stated it was "*unacceptable for banks and other organisations to carelessly discard their customers' information*", and that "*[i]ndividuals must feel confident that banks and other organisations are safeguarding their personal information*". The ICO stated it would take further enforcement action against these companies if they fail to comply with their undertaking, and these companies should carry out an audit of their information security systems.

Other security breaches

Halifax, Nottinghamshire Teaching Primary Care Trust, and TKMaxx also all found themselves the subject of unwanted publicity as a result of serious security breaches.

A computer printout containing the names of around 13,000 Halifax mortgage customers was stolen from the car of a Halifax employee, together with address, mortgage account number and balance details on the print out. On (presumably, coincidentally) the same evening, laptops were stolen from the offices of Nottinghamshire Teaching Primary Care Trust (PCT). They contained the names, address and date of birth of children aged between 8 months and 8 years old in certain areas of Nottinghamshire. Access to this information was protected by password only. The PCT stated it has written to the families affected (of which there are almost 10,000) to notify them of the theft, and set up a helpline to provide further information. Lastly, the parent company of T.K.Maxx, TJX, recently announced it discovered that it suffered breaches of its computer security systems both in the US and in the UK relating to more than 45 million credit and debit cards used in transactions in, and customers who returned goods without a receipt to, its U.S., Puerto Rico and Canada stores.

No Security Notice Breach Requirement in the UK

These cases have reopened a debate as to whether there should be a requirement on those handling personal data to inform customers (the data subjects) of any security breach when that has occurred, which is not the law in the UK, but is the position in some US States. As it turns out, organisations do when suffering such breaches sometimes nonetheless voluntarily decide to notify customers/individuals. Enforcement agencies may well take such action into account when determining sanctions. For instance, Nationwide wrote to all 11 million of its customers, which was a factor relevant to the action taken by the FSA, although it is not clear whether Nationwide actually wrote as a result of a request by the FSA.

Key Points for Financial Institutions (and indeed others)

These cases are a salutary reminder of the need for proper security. For FSA regulated firms, the 2004 Information Security report remains essential reading for firms; and such firms should keep their security procedures up to date. Key points are that firms should :-

- ensure they have adequately assessed risk regarding the security of their customer information;
- put in place procedures to manage this risk, and controls to ensure that procedures are followed;
- train and monitor employees in relation to their information security procedures; and in relation to dealing with emerging threats;
- ensure they have management procedures to deal with the loss of IT equipment or other security breaches. These procedures should provide for rapid investigation into the nature of the breach (what data was compromised), incident management commensurate with the size of the operation and nature of the breach, rapid rectification, and reporting and handling by the appropriate level of senior management. The procedures should be adequately tested, and continually enhance following experience.

Practice group contacts

For more information, please contact one of the lawyers listed, or the Dechert lawyer with whom you regularly work. Visit us at www.dechert.com.

Sarah Delon-Bouquet
Paris
+33 1 53 65 05 12
sarah.delon@dechert.com

Olaf Fasshauer
Munich
+49 89 21 21 63 21
olaf.fasshauer@dechert.com

Renzo Marchini
London
+44 20 7184 7563
renzo.marchini@dechert.com

Giovanni Russo
Munich
+44 20.7184.7310
giovanni.russo@dechert.com

Jean-Yves Steyt
Brussels
+32 25 35 54 25
jean-yves.steyt@dechert.com

Benedikte Verdegem
Brussels
+32 2 535 5440
benedikte.verdegem@dechert.com

Dechert LLP

www.dechert.com

UK/Europe	US	
Brussels	Austin	Newport Beach
London	Boston	Palo Alto
Luxembourg	Charlotte	Philadelphia
Munich	Harrisburg	Princeton
Paris	Hartford	San Francisco
	New York	Washington, D.C.