

Christopher Kuner

**European Data Protection Law:
Corporate Compliance and Regulation**

Oxford University Press

Internet Update 2.0/April 2008

New materials since the last update are enclosed in a box

Chapter 5

Paragraph 5.26

On 8 March 2007, the French data protection authority (CNIL) refused to authorize the creation of a centralized database on credit granted to individuals that would allow banks and financial institutions to share information about their clients and their credit facilities. The grounds for refusal included in particular: (1) the absence of a legal basis that would legitimize the transfer of data covered by bank secrecy to a data processor not subject to the same obligation; (2) disproportionality between the processing and its purposes, namely disclosure of detailed information; risk of profiling and extensive retention periods; and (3) the requirement that credit applicants sign a clause whereby they agreed to the lifting of banking secrecy without being fully informed about the consequences of their signing such a clause.¹

Paragraph 5.28

On 25 April 2007, the CNIL decided that information relating to suspicious transactions transferred to Tracfin (a service of the French Ministry of Finance fighting money laundering) can be shared between designated personnel of divisions of the same corporate group providing financial services situated on French territory. In addition, personal data used to fight money laundering and terrorism financing may be transferred more widely between designated personnel of divisions established on the territory of the European Union, the European Economic Area or the territory of the state that, by the Commission's determination, ensures an adequate level of protection, provided that the financial authority of that state concluded a bilateral convention of cooperation with the French Banking Commission. The decision modifies the simplified authorization no AU-003 (Decision No. 2005-297 of 1 December, 2005) that did not provide a possibility of sharing information on suspicious data between companies belonging to the same corporate group.²

Paragraph 5.62

In an opinion released on 13 March 2007, the Independent Center for Data Protection of the German federal state of Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz — ULD) set out its position regarding human resources surveys by employers. Under the German Federal Data Protection Act, the collection and processing of personal data is prohibited unless it is based on the data subject's prior consent or on a legal basis provided in the Act. The opinion by the ULD describes the

¹ See 'La CNIL refuse la création d'un fichier central de crédit', 8 March 2007, available at <http://www.cnil.fr/index.php?id=2209&print=1>.

² Decision No 2007-060 of 25 April 2007, press release (in French only) available at: <http://www.cnil.fr/index.php?id=2224>.

application of the different legal bases (consent, employment contract, legitimate interest, collective agreement) and concludes that only a questionnaire which is conducted in full anonymity is in compliance with data protection law. The opinion outlines the appropriate requirements to ensure anonymity.³

Paragraph 5.67

Consent of trade unions may be required for employee monitoring in Italy.⁴ The Italian DPA has also issued guidelines for employee monitoring.⁵

Paragraph 5.68

The European Court of Human Rights has recognized that monitoring of employee communications may be legitimate under certain circumstances.⁶

Paragraph 5.84

The importance of adopting a formal policy for employee monitoring is demonstrated by the *Case of Copland v. The United Kingdom*.⁷ In that case, the European Court of Human Rights declared partially admissible the claim of the employee of a public body, who claimed that e-mails she had sent from work and her personal internet usage had been improperly monitored by her employer. The Court based its ruling in part on the fact that the employer had not adopted a formal policy on employee monitoring.⁸

³ See 'Datenschutzrechtliche Aspekte bei der Durchführung einer Mitarbeiterbefragung', 13 March 2007, <https://www.datenschutzzentrum.de/wirtschaft/praxis/20070313.htm>.

⁴ See Linkomies, 'Employee monitoring in Italy often requires trade union consent', (August 2006) *Privacy Laws & Business International Newsletter* 21.

⁵ 'Provvedimento: Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori'. (GU n. 58 del 10-3-2007), available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522>. See Del Ninno, 'Italy: recent developments in data protection--guidelines on the processing of employee personal data by employers within the private sector', (February 2007) *BNA World Data Protection Report* 3.

⁶ See *Case of Copland v. The United Kingdom*, Application no. 62617/00 (3 April 2007) ECHR, para. 48, stating 'The Court would not exclude that the monitoring of an employee's use of a telephone, e-mail or internet at the place of work may be considered 'necessary in a democratic society' in certain situations in pursuit of a legitimate aim'.

⁷ Ibid.

⁸ See para. 42, stating 'The applicant in the present case has been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone...The same expectation should apply in relation to the applicant's e-mail and internet usage.'

Paragraph 5.93

On 7 March 2007, the French labor minister announced a consultation with trade unions and businesses about reforming the French Labor Code to allow for the implementation of whistleblower hotlines at the workplace. The announcement follows a report prepared by the University of Montpellier and AREVA Groupe, calling the Government to amend the Labor Code to introduce specific provisions to regulate the use of whistleblower systems by employees. The report proposes to restrict the use of whistleblower systems to the following three categories of infringements: (1) acts contrary to the law, labor agreements, or ethics and business rules, which would seriously harm the functioning of the company; (2) infringement of the rights of individuals and personal liberties; and (3) harm to the mental and psychic health of employees. The report also underlines that a whistleblower hotline should be introduced in the company via labor agreements; should define the practical rules of the system, such as whether the report is made anonymously or confidentially; and should provide for the guarantees against any retaliation for the use of the system in good faith.⁹

Paragraph 5.95

On 24 April 2007, the conference of German federal and state data protection authorities (*Düsseldorfer Kreis*) issued a set of guidelines for the use of whistleblowing hotlines.¹⁰

DPA's in other Member States have also issued guidance on whistleblower hotlines, including the following:

- On 29 November 2006, the Belgian DPA issued guidelines on the use of whistleblower hotlines.¹¹
- On 1 January 2007, new whistleblower provisions adopted by the Norwegian DPA entered into force.¹²

⁹ The press release and the full text of the report can be found (in French only) at:

http://www.lefigaro.fr/eco/20070307.FIG000000076_gerard_larcher_veut_encadrer_la_delation_au_travail.html.

¹⁰ 'Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz', available (in German) at <http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationssystem/wirtschaft/whistleblowing.html>.

¹¹ See 'Recommandation relative à la compatibilité des systèmes d'alerte interne professionnelle', available both in French and Dutch at <http://www.privacycommission.be/communiqués.htm>.

¹² A summary is available in English at http://www.datatilsynet.no/templates/Page_1857.aspx.

- In the summer of 2007, the Spanish DPA adopted a paper regarding the implementation of whistleblower systems in companies.¹³

Broadly speaking, all the various DPA guidelines follow the guidance of the Article 29 Working Party, with some variants.

Paragraph 5.119

In another case in Germany, a company offered an online lottery, and in the course of the online registration made its terms and conditions available for viewing by customers via a pop-up window on the user's screen. However, the user had installed software that blocked pop-ups, so that he was unable to view the terms and conditions. The user later sued the company on the basis that its terms and conditions were invalid, since the company had not provided the information to users that was required by consumer protection legislation. The German court agreed with the user, and issued an injunction against use of the pop-up procedure.¹⁴

Paragraph 5.126

On 12 December 2007, the Spanish Data Protection Agency (AEPD) published a report analyzing the privacy policies of major Internet search engines and calling for limits on search data storage and e-mail filters.¹⁵ The report, entitled 'Declaration on Internet Search Engines', is the result of information provided by Google, Microsoft and Yahoo!. It reveals significant differences between companies' privacy policies and a lack of information to consumers on how their personal data is being used. Moreover, the report states that although companies may not store personal data for longer than necessary to provide the intended services or for limited functions such as service improvement, they currently retain search data between 13 and 18 months. Additionally, the AEPD criticized e-mail services that scan mail to offer personalized advertising, since scanning is only permitted to filter spam and viruses. The Declaration also targeted the registration data required of consumers in order for them to create blogs or use other Internet services. Therefore, the Agency asked the search engine companies to develop new information mechanisms providing clear and visible information to customers on how their data is used, and giving them the right to cancel, correct, or challenge it.

Paragraph 5.135

¹³ Informes jurídicos No. 2007-0128, available (in Spanish) at https://www.agpd.es/upload/Canal_Documentacion/Informes%20Juridicos/Otras%20cuestiones%20de%20interes/OC%20%282007-0128%29%20%28Creaci%F3n%20de%20sistemas%20de%20denuncias%20internas%20en%20las%20empresas%2C%20mecanismos%20de%20whistleblowing%29.pdf.

¹⁴ Oberlandesgericht Düsseldorf, Urteil vom 13. April 2006, no VI-U(Kart) 23/05.

¹⁵ The Declaration on Internet Search Engines is available (in Spanish) at: https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/declaracion_aepd_buscadores.pdf.

There are many EU instruments (some with legal force and some without) that have an impact on information security issues, besides instruments of data protection law. The European Network Security Agency (ENISA) has published a survey of such instruments.¹⁶

Paragraph 5.140

The number of security breach incidents in Europe (or at least the number of incidents that become publicly known) seemed to increase dramatically in 2007, as is demonstrated by the following examples:

- In early 2007, the Swedish broadband provider Bredbandsbolaget was under investigation by the Swedish National Post and Telecom Agency (PTS) for compromising the security of the usernames and passwords of its subscribers. In late 2006, the company had carried out an advertising campaign in connection with its merger with the telecommunications company Telenor. The campaign involved sending out pamphlets to a large number of the provider's customers, which included each customer's usernames and passwords in the pamphlets, which were folded and sealed with glue. However, it seems that it was easy to display the username and passwords just by bending the pamphlet slightly, which in effect gave easy access to the customers' accounts. It was also revealed that the information on Bredbandsbolaget's servers was kept unencrypted. The company was forced to issue a public apology, and a number of complaints were made to the PTS, which declared that the company was in breach of data security requirements.
- On 4 January 2007, the French Data Protection Authority (CNIL) announced that leading Internet service provider Free SAS had erroneously transferred personal data, including unlisted phone numbers, from more than 120,000 customers to third-party operators of web-based and phone-based directory services. Complaints were made to the CNIL in May and June 2006 by Free SAS subscribers who had objected to the disclosure of their phone numbers to public phone directories. After Free SAS explained that this was due to an error in its IT system programming, the CNIL took the position that Free SAS had committed a serious infringement of its security obligations under Article 34 of the French Data Protection Act. The CNIL decided not to impose any fines as it was satisfied that Free SAS took measures to correct its internal security controls. The CNIL however considered that this was a particular threat to privacy which justified a public warning. The CNIL also reminded all telecom operators of their duty to ensure data security and to enforce individuals' data protection rights, including

¹⁶ ENISA ad hoc working group on regulatory aspects of network and information security (RANIS), 'Inventory and assessment of EU regulatory activity on network and information security (NIS)' (December 2006), available at http://www.enisa.europa.eu/pages/ENISA_Working_group_RANIS.htm. The author was one of the members of the ENISA working group that drafted the report. See para 1.25 below regarding ENISA.

their rights to object to the inclusion of their data in such lists or to correct their data.¹⁷

- In January 2007, the Greek Authority for the Information and Communication Security and Privacy fined Vodafone €76 million over a security breach and wiretapping scandal involving the illegal monitoring of the mobile calls of top government officials such as the Prime Minister and the Foreign Minister. Vodafone was ruled at fault for not preventing unknown hackers from subverting a legitimate surveillance system, supplied by Ericsson, to spy on Greek officials around the time of the 2004 Athens Olympics. Calls from and to targeted phones were relayed to sixteen mobile phones using pre-paid cards, located in central Athens, thanks to unauthorized manipulation of the Ericsson-supplied surveillance software used by Vodafone Greece. The Authority said that Vodafone had failed to take adequate measures to protect its network and had not informed subscribers that their phones were being tapped. It further criticized Vodafone for obstructing its investigation by failing to admit the existence of the surveillance system itself.
- In February 2007, the UK financial services regulator, the Financial Services Authority (FSA), fined the UK's largest building society, Nationwide, £ 980,000 following the theft of an employee's laptop.¹⁸ The laptop contained customer data relating to some of its eleven million account holders. The FSA criticised Nationwide for failing to adequately address the risk that customer data might be lost or stolen. The laptop was stolen from the home of a Nationwide employee who reported the theft but not the fact that the laptop contained such a significant amount of customer data. The employee then went on holiday for three weeks. During this period nothing was done to investigate what data the stolen laptop contained. The FSA indicated that Nationwide's risk assessment and security procedures were inadequate. The FSA specifically pointed to the fact that staff members did not know what steps they were supposed to take in the event of such a breach. Policies were inaccessible and staff were not adequately trained. The fact that no action was taken in the first three weeks after the breach increased the opportunity for the information to be misused. Of particular importance is the fact that Principle 11 of the Principles for Business section of the FSA Handbook requires regulated firms to deal with regulators in an open and cooperative way, and to disclose to the FSA anything relating to the firm of which the FSA would reasonably expect notice; the FSA's action seems to indicate that it regards data security breaches as falling within this obligation, at least to the extent that a security breach indicates a wider, systematic problem in relation to part of the firm's internal controls.
- On 13 March 2007, the UK Information Commissioner found eleven banks and other financial institutions in breach of the Data Protection Act after investigating

¹⁷ The CNIL's decision can be found (in French) at <http://www.cnil.fr/index.php?id=2165>.

¹⁸ Further information is available at <http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml>. See B Treacy, 'Nationwide: movements towards a notification regime', (February 2007) Data Protection Law and Policy 4.

complaints concerning the careless disposal of customer information.¹⁹ The Commissioner required these organizations to sign a formal undertaking to comply with the principles of the Data Protection Act. The Commissioner stated that organizations in breach of the Data Protection Act security requirements will face a detailed inspection of their security procedures.

- On 12 November 2007, the UK Information Commissioner's Office published a formal undertaking whereby the Foreign Office committed itself to comply with the principles of the Data Protection Act in the future. The Foreign Office entered into such commitment following a security error that occurred on its website in May 2007. This error resulted in the personal data of individuals in India, Russia and Nigeria applying for an entrance visa to the UK becoming visible to other Internet users and easily accessible to hackers. The ICO launched an investigation which led to severe criticisms of the Foreign Office's outsourcing practices and management. In particular, the ICO criticized the decision of the Foreign Office to outsource its Internet processing to a firm that is not an IT specialist, and the failure by the Foreign Office to respond adequately when the security breach was initially disclosed in December 2005.²⁰
- On November 20 2007, Chancellor of the Exchequer Alistair Darling announced in an address to the House of Commons that discs containing personal data on some 25 million citizens of the United Kingdom had been lost in the mail when tax officials sent the information to government auditors for review. The lost data relates to Child Benefit, a universal social welfare payment paid to the parent or caregiver of children. The Information Commissioner's Office characterized this data breach as 'extremely serious and disturbing.'²¹
- On 17 December 2007, the UK Financial Services Authority (FSA) fined Norwich Union Life £1.26 million for neglecting to put in place effective systems and controls to protect customers' confidential information. Because of the weakness of the Norwich Union Life system, fraudsters were able to use publicly available information such as names and birthdates to impersonate customers and obtain sensitive customer details from its call centers. The FSA found out that the company had failed to properly assess the risks of financial crime and therefore its customers were more likely to fall victim to such crimes. Norwich Union settled at the early stage of the investigation and also reinstated its policies in full.

¹⁹ Further information is available at http://www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf.

²⁰ The full text of the formal undertaking is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/notices/foreign%20_commonwealth_office.pdf.

²¹ The full text of Mr. Darling's statement is available on the Treasury Web site at http://www.hm-treasury.gov.uk/newsroom_and_speeches/speeches/statement/speech_statement_201107.cfm and the reaction of the ICO is available at http://www.ico.gov.uk/upload/documents/pressreleases/2007/personal_details_lost_by_hmrc_201107003.pdf.

These incidents illustrate the significant financial, legal, and reputational risks associated with breaches of data security requirements.

Paragraph 5.148

Norway has enacted legislation which includes an explicit duty to notify the Norwegian Data Inspectorate when certain information security breaches occur. Paragraph 1 of Section 2-6 of the Norwegian Personal Data Regulations defines ‘any use of an information system that is contrary to established routines, and security breaches’, as a ‘discrepancy’. Paragraph 3 of the same section then provides that ‘if the discrepancy has resulted in the unauthorised disclosure of personal data where confidentiality is necessary, the Data Inspectorate shall be notified’. The provision does not provide that the respective data subjects must be notified, only the Data Inspectorate.

Some Member States have established governmental agencies dealing with information security. Such agencies typically cooperate with the respective national data protection authority, and other relevant authorities, on information security issues. An example of such an authority is the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* or BSI), which has existed since 1989. Italy also established the ‘Authority for Information and Security Systems’ (*Autorità delegata al sistema di informazione e sicurezza*) in February 2007.

Paragraph 5.151

The security breach in the Postbank case also led to a class action suit being brought in the US in February 2007. The suit was brought by an individual in Germany who had a credit card issued by the German bank Commerzbank. In 2006 the individual was investigated by the German police for allegedly purchasing child pornography online, since such material had been purchased with his credit card. However, the investigation failed to find any evidence that the individual was involved in the purchase, and the police eventually cleared him. It was only after conclusion of the police investigation that Commerzbank informed the individual that his credit card had been compromised in the Postbank security breach in the US, which was over a year after the bank became aware of the breach. The individual then brought a class action suit in the US against Commerzbank, and even placed an advertisement in a leading German newspaper seeking other individuals whose data might have been compromised to join him in the suit. This case demonstrates that security breaches involving the personal data of EU citizens may also have legal consequences outside the EU, and that a failure to notify individuals of security breaches in a timely fashion carries legal risks.²²

²² An overview of dealing with security breaches is provided by A Simpson and L Sotto, ‘A How-To Guide to Information Security Breaches’, (2 April 2007) *BNA Privacy Reporter* 559.