

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

Appendix 13

Selected Enforcement Measures in EU Member States and Article 29 Working Party from September 2002- UPDATED APRIL 2008

Country/ Entity	Measure	Link
France	<p>May 2007 <i>CNIL Imposes € 30,000 fine on Tyco Healthcare France.</i> In May 2007, the French Data Protection Authority (CNIL) published its Decision 2006-281 of 14 December 2006 imposing a €30,000 fine on Tyco Healthcare France for inadequate reports to the CNIL over international transfers of HR data. Further to notifying its international HR management processing, Tyco had been summoned by the CNIL to provide additional information, in particular about the purposes of the data transfers outside France, the location of the servers and systems, the recipients of the data and the security measures taken to protect the confidentiality of the data. Tyco informed the CNIL that the data processing had been suspended, but an investigation at Tyco's premises revealed that it was still taking place, and that its purposes exceeded the ones declared in the notification. In December 2006, the CNIL therefore sanctioned Tyco with a €30,000 fine for failure to cooperate and for lack of transparency.</p>	<p>Further information (in French only) is available at: http://www.cnil.fr/index.php?id=2206&news[id]=440&cHash=3c7837cb1e</p>

	<p>28 May 2007</p> <p><i>CNIL Imposes Heavy Fine on Crédit Agricole for Irregular Blacklisting.</i> On 28 May 2007, the CNIL published its Decision 2006-245 of 23 November 2006 imposing a €20,000 fine on Crédit Agricole for wrongly listing clients on the nationwide blacklist (Fichier national des incidents de remboursements des crédits aux particuliers — FICP) maintained by the Banque de France. The case involved a couple of individuals who were added to the blacklist sixteen years after the payment incident had occurred and was subsequently resolved. Further to an amicable procedure, the CNIL requested that the bank remove the individuals from the FICP. The bank, however, inadvertently listed them a second time. Summoned by the CNIL to implement organizational and technical guarantees to prevent similar errors in the future, the bank failed to communicate to the CNIL any appropriate measures. The bank was fined €20,000 for failure to take adequate safeguards to protect the rights of the individuals concerned.</p>	<p>The press release is available at: http://www.cnil.fr/decision/decision.php?id=2225&fcbdcfcbe</p>
	<p>12 December 2007</p> <p><i>Google Fined by French Court.</i> On 12 December 2007, the Paris Court of Appeal ruled that web-hosting services must be able to fully identify the editors and operators of blogs and other personal sites and may not rely on Internet Protocol addresses as their principal personal identifier. In mid-2006, Benetton had asked Google to block access to blogs on their hosting services that Benetton accused of violating the company's trademark. Google refused to do so. On March 1 2007, the Paris Court of First Instance ordered Google to forward to Benetton personal data on the identity of the individual behind the fraudulent website. Google responded by forwarding an e-mail address and two IP addresses. The Paris Court of First Instance considered this response unsatisfactory and issued an emergency injunction demanding an immediate ban on the blog. Despite Google's appeal, the Paris Court of Appeal upheld this decision and ordered Google to pay to Benetton €36,000 in damages for failing to comply with French rules on web-hosting.</p>	<p>The Court's opinion is available (in French) at: http://www.legalis.net/jurisprudence-decision.php3?id_article=2116</p>

Germany	<p>3 September 2007</p> <p><i>DPA Send Compliance Questionnaire to 1,000 Companies.</i> On 3 September 2007, the DPA of the Federal State of Mecklenburg-Vorpommern began a survey on some 1,000 companies in all industry sectors concerning their compliance with data protection law. The questionnaire addresses the handling of customer, supplier and employee data.</p>	<p>The press release is available at: http://www.datenschutz-mv.de/dschutz/presse/pmgrunddaten.pdf</p>
	<p>21 December 2007</p> <p><i>Federal DPA Audits 26 Telecommunications Companies.</i> In a press release, the German Federal DPA stated that it had recently audited 26 telecommunications companies in Germany, and discovered a variety of legal violations. It also said that the companies had to change their practices, or further enforcement action would be taken.</p>	<p>Press release available (in German only) at www.bfdi.bund.de</p>
Netherlands	<p>18 December 2007</p> <p><i>Telecommunications Regulator Imposes Large Fine for Spyware.</i> On 18 December 2007, the Dutch independent authority regulating postal and electronic communications services (Onafhankelijke Post en Telecommunicatie Autoriteit — OPTA) imposed a fine totaling €1,000,000 on three Dutch companies operating under the name DollarRevenue. These companies had surreptitiously installed spy- and adware on over 22 million computers belonging to Internet users in the Netherlands and elsewhere. This practice allowed them to spy on consumers' online behavior and triggered pop-up windows with advertising material.</p>	<p>For additional information, please consult these press releases (in English) at: http://www.opta.nl/asp/en/newsandpublications/pressreleases/document.asp?id=2459</p>

<p>Spain</p>	<p>17 April 2007</p> <p>On 17 April 2007, the Spanish Supreme Court affirmed the €1,081,822 fine imposed in January 2001 by the Spanish Data Protection Authority on Zeppelin Television S.A., which produces the Spanish version of the ‘Big Brother’ television reality show, under the title ‘Gran Hermano’ (see para. 1.88 above). In 2001, the Spanish DPA had launched an investigation against Zeppelin following access by internet hackers to personal data of some 7,000 potential contestants on the show, and their subsequent publication on an unofficial website dedicated to the show. In some cases, the accessed personal data revealed information about potential contestants’ racial origin, religious beliefs, health and sex life. Zeppelin unsuccessfully tried to convince the DPA that it had fallen victim to illegal hacking activities. The DPA found Zeppelin in breach of the provisions of the Spanish Data Protection Act and imposed the highest fine to date in Spain in a single administrative proceeding. This decision was later confirmed by the Spanish National High Court in its ruling of January 2003, which was then challenged by the defendant. The Spanish Supreme Court found Zeppelin in breach of the provisions of the Data Protection Act (1) for failure to obtain the contestants’ express consent for the processing of sensitive data; (2) for failure to obtain the individuals’ express consent to the disclosure of their personal data to third parties; and (3) for failure to implement the technical and organizational measures necessary to ensure the security of the personal data and to prevent their alteration, loss, or unauthorized processing or access.</p>	<p>The full text of the decision is available (in Spanish) at: http://www.poderjudicial.es/jurisprudencia/pdf/28079130062007100141.pdf?formato=pdf&K2DocKey=E:\Sentencias\20070531\28079130062007100141.xml@sent_supremo&query=%28Zeppelin%29</p>
<p>United Kingdom</p>	<p>13 March 2007</p> <p><i>Information Commissioner Finds Eleven Banks in Breach of Data Protection Act.</i> On 13 March 2007, the Information Commissioner found eleven banks and other financial institutions in breach of the Data Protection Act after investigating complaints concerning the careless disposal of customer information. The Commissioner has now required these organizations to sign a formal undertaking to comply with the principles of the Data Protection Act. Failure to meet the conditions of the undertaking is likely to lead to further enforcement action by the Commissioner. The Commissioner stated that organizations in breach of the Data Protection Act security requirements will face a detailed inspection of their security procedures.</p>	<p>The press release is available at: http://www.ico.gov.uk/upload/documents/press_releases/2007/banks_in_unacceptable_data_protection_breach.pdf</p>

	<p>17 December 2007</p> <p><i>FSA Levies Large Fine for Security Breach.</i> 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.</p>	<p>The full text of the notice about a financial penalty is available (in English) at: http://www.fsa.gov.uk/pubs/financial/Norwich_Union_Life.pdf</p>
	<p>16 January 2008</p> <p><i>Information Commissioner Takes Action against Carphone Warehouse.</i> The ICO found Carphone Warehouse, and its sister company TalkTalk, in breach of the Data Protection Act after investigating complaints concerning the way in which both organisations processed and stored personal information. The ICO ordered Carphone Warehouse and TalkTalk to improve their data protection practices or face prosecution after both companies failed to meet the basic principles of the Data Protection Act. The investigation revealed that Carphone Warehouse and TalkTalk had been opening customer accounts in the wrong name and passing inaccurate information on to credit reference agencies and debt collection agencies. Security failings had also led to customers being able to view other customers' account details online. In addition, the ICO found that the companies had not responded to requests by individuals for information held about them.</p>	<p>The press release is available at http://www.ico.gov.uk/about_us/news_and_views/press_releases.aspx</p>