

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 1

Paragraph 1.01

More and more countries outside of Europe are adopting data protection laws which show the influence of the European model. A good example is the Dubai International Financial Centre (DIFC), which in 2007 adopted a Data Protection Law closely modeled after the General Directive.¹ The Spanish Data Protection Authority has also established an 'Iberoamerican Data Protection Network', which helps promote the European approach to data protection in Latin and South America.

Paragraph 1.07

On January 1 2007, Bulgaria and Romania acceded to the European Union. Thus, the EU is currently made up of 27 Member States.

Paragraph 1.15

On 29 January 2008, the European Court of Justice rendered its judgment in the case of *Productores de Música de España (Promusicae) v. Telefónica de España SAU*.² The Court found that the EU Member States are not obliged under Community law to require disclosure of personal data in the context of civil proceedings for the purpose of copyright protection, but that they may require such disclosure, and that in transposing the various directives on intellectual property, e-commerce and data protection, Member State must strike a fair balance between the fundamental rights that they protect, and must respect general principles of Community law, such as the principle of proportionality.

Paragraph 1.25

See para 5.135 below regarding a study published by ENISA on EU instruments that have an impact on information security issues.

Paragraph 1.33

In November 2007, the European Commission sued the government of Germany before the European Court of Justice because of a lack of independence of German federal state DPAs.³

¹ DIFC Data Protection Law 2007.

² *Productores de Música de España (Promusicae) v. Telefónica de España SAU* (Case C-275/06) [2008], available at <http://curia.europa.eu>.

³ Action brought on 22 November 2007 -- Commission of the European Communities v Federal Republic of Germany, Case C-518/07 [2008] OJ C37/8.

One commentator has noted that ‘funding for enforcement of the European Union’s complex and stringent data protection law varies widely within the 27 EU Member States, leading to uneven results for businesses across the Continent...’⁴

Paragraph 1.35

In a landmark judgment handed down on 27 February 2008, the German Federal Constitutional Court placed severe restrictions on the law enforcement monitoring of online activities and private computer usage. Finding that monitoring computer use creates even greater dangers to privacy than does wiretapping telephone use or bugging private homes (since it allows the creation of comprehensive personal profiles), the Court created a new fundamental right of computer privacy. While the case applies directly only to law enforcement activities, its wide-ranging nature means that it will probably also further limit the ability of companies to carry out such activities as monitoring employee computer usage and creating customer profiles.⁵

Paragraph 1.56

On 19 March 2007, the German Federal Constitutional Court issued a preliminary injunction on data protection grounds which will result in substantial changes to the legislation proposed by the government to implement the EU Data Retention Directive.⁶ While the Court refused to block implementation of the Directive in Germany, it substantially limited the scope of the uses to which data stored pursuant to the implementing legislation may be put, ruling that they may only be used to prosecute certain types of serious crimes (*schwere Straftaten*) such as murder, kidnapping, money laundering etc. In addition, the Court ordered the government to present evidence regarding the practical effects of data retention, and indicated that it will examine the constitutionality of data retention in its upcoming ruling (which is, however, not likely before 2009). The legislation originally proposed by the German government to implement the Directive would have permitted a much broader use of stored data than the Court allowed.

Paragraph 1.70

On 2 May 2007, the European Commission adopted a communication identifying the benefits of Privacy Enhancing Technologies (PETs) and laying down the Commission’s objectives in this field, to be achieved by a number of specific actions supporting the development of PETs and their use by data controllers and consumers.⁷

⁴ L Speer, ‘Variable Funding of EU Privacy Law Means Uneven Enforcement Across European Union’ (January 2007) *World Data Protection Report* 24.

⁵ Bundesverfassungsgericht, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 595/07.

⁶ Bundesverfassungsgericht, Beschluss vom 11. März 2008, 1 BvR 256/08.

⁷ Available at http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf.

Paragraph 1.74

On 16 February 2007, the DPA of the German federal state of Schleswig-Holstein awarded its privacy seal to the Windows online update procedure of Microsoft.⁸

Paragraph 1.77

The European Union and the European data protection authorities work closely with the Council of Europe in the areas of fundamental freedoms and data protection, and the EU has committed to ensure that European law is consistent with the relevant conventions of the Council of Europe (though European law may provide more extensive protection).⁹

Paragraph 1.82

On 20 June 2007, the Article 29 Working Party published a report on its first joint enforcement action.¹⁰ The action included a joint investigation of data controllers in the private health insurance sector carried out by the DPAs of Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovenia, the Slovak Republic, Spain, Sweden, and the United Kingdom.¹¹ The investigation lasted thirteen months, and the Working Party found the results to be 'positive', noting that 'one can assume that, in general, the processing of personal data by the private health insurance companies is in compliance with the principles and provisions laid down in Directive 95/46/EC on the protection of personal data'.¹² At the same time, the Working Party announced its intention to carry out further such joint investigations, noting that they should 'become more like true audit actions, which require the power to directly verify the truthfulness of responses. It is furthermore necessary to institute random checks on the selected data controllers as an integral part of such investigations'.¹³ The Working Party also noted that the sectors to be examined in such audits would be selected based on an assessment of the data protection risks the sector poses, and the advantages of undertaking co-ordinated action at a European level.¹⁴

⁸ See J Bizer, 'Microsoft erhält für Updateverfahren Datenschutz-Gütesiegel' (2007) *Datenschutz und Datensicherheit* 76.

⁹ See Memorandum of Understanding between the Council of Europe and the European Union paras. 27-19, May 2007.

¹⁰ Article 29 Working Party, 'Report 1/2007 on the first joint enforcement action: evaluation and future steps' (WP 137, 20 June 2007).

¹¹ *Ibid*, 4.

¹² *Ibid*, 7.

¹³ *Ibid*, 8.

¹⁴ *Ibid*.

On 28 June 2007, the United States Department of the Treasury issued various representations describing controls and safeguards that the Treasury commits to use in accessing the SWIFT database.¹⁵ In a joint letter in reply, the European Commission and the Council of the European Union stated that ‘Once SWIFT and the financial institutions making use of its services have completed the necessary arrangements to respect EC law, in particular through the provision of information that personal data will be transferred for commercial purposes to the United States and, as regards SWIFT, the respect of the ‘Safe Harbour [sic]’ principles, subject to lawful access by the US Treasury Department, SWIFT and the said financial institutions will be in compliance with their respective legal responsibilities under European data protection law.’¹⁶

Paragraph 1.88

On 15 June 2007, SWIFT announced that it would change the architecture of its data processing system so that intra-European data would be stored only in Europe (rather than in the US as was previously the case).¹⁷ While, strictly speaking, this cannot be considered an ‘enforcement action’, the change of architecture does demonstrate how EU data protection law can influence business decisions.

Paragraph 1.94

Sweden has gone the furthest in taking into account in its regulatory framework the criticisms that have been made of data protection law. In amendments to the Swedish Personal Data Protection Act that entered into force on 1 January 2007, the Act was made inapplicable to unstructured data sets, except in cases where personal integrity is violated. The exemptions to notifying data processing to the data protection authority were also expanded. These changes will likely make it easier for data controllers to operate in Sweden.

Paragraph 1.97

On 7 March 2007, the European Commission adopted a communication on the work program for better implementation of the General Directive which the Commission had adopted in 2003.¹⁸ In its Communication, the Commission concluded that

¹⁵ Letter from United States Department of the Treasury regarding SWIFT/Terrorist Finance Tracking Programme [2007] OJ C166/17.

¹⁶ Reply from European Union to United States Treasury Department-- SWIFT/Terrorist Finance Tracking Programme [2007] OJ C166/26.

¹⁷ See SWIFT press release at http://www.swift.com/index.cfm?item_id=62260.

¹⁸ Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Commission document COM(2007) 87 final.

implementation of the Directive had improved, although some Member States had still not properly implemented it.¹⁹ The Commission also stated that the Directive should not be amended.²⁰ Finally, the Commission noted several areas where it would work to improve implementation of the Directive, including the following: (1) continuing to work with Member States to ensure improved implementation; (2) producing interpretative communications on some provisions of the Directive; (3) encouraging all actors to reduce national divergences in implementation; (4) reviewing the impact of new technologies on data protection; and (5) dealing with the challenges posed by the demand for data processing based on public interest, particularly relating to law enforcement. On 25 July 2007, the European Data Protection Supervisor issued an opinion on the Commission's Communication which supported the Commission's conclusion that the Directive should not be amended at this time, but which seemed to see a more urgent need to improve its implementation by the Member States.²¹ In particular, the EDPS emphasized the importance of: (1) full implementation of the Directive; (2) considering the impact of technological developments on the Directive; (3) having a global perspective and further developing rules on international data transfers; (4) ensuring that personal data are protected despite law enforcement demands; (5) adopting more sectoral data protection legislation (for example, regarding RFID); (6) greater use of infringement procedures against the Member States; (7) encouraging the use of interpretative communications by the Commission to clarify important questions; (8) enhancing the use of non-binding instruments to increase compliance, such as privacy seals; and (9) better defining the role of institutional actors, in particular the Article 29 Working Party.

¹⁹ Ibid, 5.

²⁰ Ibid, 9.

²¹ 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive', available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf.