

Chapter 1

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 1.25

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 August 2007, the European Commission announced that it was planning to sue the government of Germany before the European Court of Justice because of a lack of independence of German federal state DPAs.

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...’¹

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.²

Paragraph 1.82

On 20 June 2007, the Article 29 Working Party published a report on its first joint enforcement action.³ 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.⁴ 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

¹ L Speer, ‘Variable Funding of EU Privacy Law Means Uneven Enforcement Across European Union’ (January 2007) *World Data Protection Report* 24.

² See J Bizer, ‘Microsoft erhält für Updateverfahren Datenschutz-Gütesiegel’ (2007) *Datenschutz und Datensicherheit* 76.

³ Article 29 Working Party, ‘Report 1/2007 on the first joint enforcement action: evaluation and future steps’ (WP 137, 20 June 2007).

⁴ *Ibid*, 4.

Directive 95/46/EC on the protection of personal data'.⁵ 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'.⁶ 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.⁷

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.⁸ 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.'⁹

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).¹⁰ While this cannot be considered an 'enforcement action', the change of architecture does demonstrate how EU data protection law can influence business decisions on a momentous scale.

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 2003.¹¹ In its Communication, the Commission concluded that implementation of the

⁵ Ibid, 7.

⁶ Ibid, 8.

⁷ Ibid.

⁸ Letter from United States Department of the Treasury regarding SWIFT/Terrorist Finance Tracking Programme [2007] OJ C166/17.

⁹ Reply from European Union to United States Treasury Department-- SWIFT/Terrorist Finance Tracking Programme [2007] OJ C166/26.

¹⁰ See SWIFT press release at http://www.swift.com/index.cfm?item_id=62260.

¹¹ 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.

Directive had improved, although some Member States had still not properly implemented it.¹² The Commission also stated that the Directive should not be amended.¹³ 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.¹⁴ 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.

¹² Ibid, 5.

¹³ Ibid, 9.

¹⁴ '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.

