

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

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

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.

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

Paragraph 1.74

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.

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

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

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.*

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 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

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.

¹⁹ Ibid, 5.

²⁰ Ibid, 9.

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.

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.

Chapter 2

Paragraph 2.19

The International Chamber of Commerce has published the minutes of a workshop on the distinction between the concepts of data controller and data processor which provides a useful summary of the issues involved.¹

Paragraph 2.25

In late 2006 and early 2007, the Article 29 Working Party adopted an opinion in the SWIFT affair,² as did a number of DPAs,³ which opinions shed light on the criteria the DPAs use to classify a company as a data controller or a data processor.

SWIFT provides secure messaging services to over 8,000 banks in over 200 countries worldwide. SWIFT has operated in Belgium since 1973 as a co-operative company (SCRL), and is owned and operated by its member financial institutions. SWIFT is itself not a bank or financial institution, nor is it regulated as such in any country. However, SWIFT is regarded by financial services regulators as ‘critical infrastructure’ and thus regularly meets with a group of central banks that act as its informal overseers.⁴ Because SWIFT is regarded as critical infrastructure, it is crucial for the stability of the global financial system that SWIFT’s database be operational at all times. In order to ensure this resiliency, SWIFT maintains two databases, one in Europe and the other in the US, in keeping with international ‘best

¹ See ICC Summary of the Workshop on the Distinction between Data Controllers and Data Processors, available at <http://www.iccwbo.org/policy/ebitt/id17704/index.html>.

² Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’ (WP 128, 22 November 2006). See paras. 1. 82 below and 4.115 above regarding the SWIFT case.

³ Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’ (WP 128, 22 November 2006), indicating that SWIFT is a data controller; Datenschutzkommission [Austria], Bescheid Beschwerde, no. K121.245/009-DSK/2007, 21 March 2007, indicating that SWIFT is a data controller for certain purposes and a data processor for others; Belgian Data Protection Commission, ‘Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas’ (unofficial translation by the DPA of AVIS N. 37/2006 du 27 Septembre 2006), indicating that SWIFT is a data controller; Independent Centre for Privacy Protection at the Federal State of Schleswig-Holstein (ULD) (Germany), Opinion of 23 August 2006 (unofficial English translation) and Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Stellungnahme zur rechtlichen Einstufung der Datenverarbeitung von SWIFT durch die Art.-29-Gruppe der Europäischen Union, 12 October 2006, both indicating that SWIFT is a data processor; Spanish Data Protection Authority, Resolución de archivo de actuaciones, Expediente No. E/00797/2006, 27 June 2007, indicating that SWIFT is a data processor.

⁴ The National Bank of Belgium is the lead overseer, and cooperates with other G-10 central banks in oversight of SWIFT.

practices' that recommend having two identical databases geographically removed from each other. The European and US databases are mirror images of each other, so that when a transaction takes place in one database, it is automatically replicated in the other one, meaning that SWIFT could continue to function were one of the two databases out of service. The SWIFT entity that maintains the US database is a branch of the Belgian parent, but is registered to do business in the US state where it operates.

One of the key services which SWIFT offers is called SWIFTNet FIN, in which SWIFT forwards messages from one company or financial institution to another one in order to effect cross-border payments. SWIFT's role in SWIFTNet FIN (which is the main service at issue) is highly limited, as SWIFT merely acts as a messenger which stores the message and then passes it on to the recipient. The only part of the message which SWIFT actually sees is the outside of the message 'envelope', which contains a limited amount of information including the date the message was transmitted, the name of the sending bank, and the name of the recipient bank. SWIFT is obliged by contract not to open a message while transmitting it, and also has limited technical ability to do so; the only exception to this is an automated validation procedure which SWIFT performs in order to determine, for example, that the correct currency codes have been used in the message. Thus, SWIFT can only, for example, search for messages sent by a particular financial institution to another institution on a particular date, but cannot search the content of messages for specific names or persons.

SWIFT's customers are banks and companies, so that it has no direct relationship with consumers or individuals. The contractual structure under which SWIFT operates makes it clear that SWIFT's role is limited to that of a data processor. All SWIFT users are bound by SWIFT's General Terms and Conditions, which state that the bank transmitting the message is the data controller and SWIFT is merely a data processor. SWIFT has also adopted a 'Data Retrieval Policy', which is supplied to customers and states that SWIFT must comply with mandatory requests from governmental authorities.

Under Article 4 of the General Directive, SWIFT is obligated to comply with Belgian data protection law since it is a data controller established in Belgium. In the view of the DPAs, this obligation to comply with Belgian law also applies to the US database, since the data entered into SWIFT's Belgian database are automatically mirrored in the US database. At the same time, as the US database is maintained on US soil, SWIFT must also comply with US law as regards this database.

Following the terrorist attacks of September 11, 2001 in the US, the Office of Foreign Assets Control (OFAC) of the US Treasury Department sought to obtain information about terrorist financing. Pursuant to the International Emergency Economic Powers Act and the United Nations Participation Act,⁵ UST thus served a subpoena on SWIFT for access to the mirrored database located in the US. After first ascertaining that the subpoena was valid under US law, SWIFT sought a way to avoid granting full access to its entire database. SWIFT was able to persuade the UST to accept a number of important restrictions on its ability to access the database, which are contained in a memorandum of understanding (MOU) between SWIFT and the UST. These protections include the following: (1) information may only be accessed by the UST regarding named individuals who are subjects of an ongoing anti-terrorism investigation, and may not be used for any other purposes; (2) SWIFT employees are on site at the UST, and have the power to halt access of the database if it exceeds the terms of the

⁵ Contrary to what has sometimes been erroneously stated, the US Patriot Act was not used as a legal basis for the subpoena.

MOU; (3) access is audited on an annual basis by a respected professional services firm engaged by SWIFT; and (4) no ‘fishing expeditions’ are allowed, i.e., the UST may only search for named and specific individuals.

The DPA opinions differ between classifying SWIFT as a data controller or a data processor. In their opinions, DPAs have used various arguments to justify classifying SWIFT as a data controller (either as a sole controller or a co-controller with the banks), such as the following:

- SWIFT management is able to determine the purposes and means of processing by developing, marketing and changing services and processing (e.g., determining standards for the form and contents of payment orders, introducing new services, etc.) without requiring the consent of banks.⁶
- SWIFT management decides autonomously on the level of information given to banks in relation to processing.⁷
- SWIFT provides added value for processing, such as the storage and validation of data and implementation of high-level security standards.⁸
- SWIFT management has the power to make critical decisions about processing (such as security standards and the location of databases).⁹
- It was not necessary for SWIFT to locate data processing in the US, so that in doing so, it exceeded its powers as a mere data processor.¹⁰
- Deeming SWIFT to be a data processor would result in the ‘scattering’ of data protection responsibility among almost 8,000 banks, which would make it impossible for individuals to have an effective recourse in the case of data protection violations.¹¹
- SWIFT negotiates and terminates with full autonomy its services agreements, and also has full autonomy to change contracts and policies.¹²

⁶ Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’, 11; Belgian Data Protection Commission, ‘Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas’, 11.

⁷ Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’, 11.

⁸ Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’, 11; Belgian Data Protection Commission, ‘Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas’, 11.

⁹ Ibid.

¹⁰ Datenschutzkommission [Austria], Bescheid Beschwerde, no. K121.245/009-DSK/2007, 21 March 2007, § 2b.

¹¹ Belgian Data Protection Commission, ‘Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas’, 12.

- SWIFT decided to comply with UST subpoenas, took the initiative to negotiate an agreement with the UST, and decided not to inform banks about the negotiations.¹³

On the other hand, DPAs have used the following arguments to support the case that SWIFT should be considered a data processor:

- Recital 47 of the General Directive provides that where a message containing personal data is transmitted via a telecommunications service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data in the message is normally considered to be the person from whom the message originates, rather than the service provider.¹⁴ This situation fits SWIFT exactly.
- SWIFT's terms and conditions support the argument that it is merely a data processor, since they clearly indicate that the banks are data controllers and that SWIFT acts on instructions from them.¹⁵
- The size of an organization or the complexity of its structure cannot be the sole grounds for qualifying it as a data controller; examples exist where the data processor is a larger organization than the data controllers that use its services.¹⁶
- The criteria for classification of SWIFT as a data controller are whether, based on the agreements between the parties, the functional decision-making power regarding the processing of personal data has in fact been transferred to the party claiming to be a processor; this is not the case in relation to SWIFT, since the service it provides consists only of the IT-based transfer and routing of standardized messages on behalf of its customers.¹⁷

¹² Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', 11.

¹³ Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', 11; Belgian Data Protection Commission, 'Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas', 12.

¹⁴ Datenschutzkommission [Austria], Bescheid Beschwerde, no. K121.245/009-DSK/2007, 21 March 2007, § 2b; Independent Centre for Privacy Protection at the Federal State of Schleswig-Holstein (ULD) (Germany), Opinion of 23 August 2006, 5.

¹⁵ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Stellungnahme zur rechtlichen Einstufung der Datenverarbeitung von SWIFT durch die Art.-29-Gruppe der Europäischen Union, 12 October 2006.

¹⁶ Ibid.

¹⁷ Ibid.

- SWIFT's role in complying with UST subpoenas does not change the analysis of its role as a data processor.¹⁸

These arguments demonstrate a considerable degree of confusion about the criteria that should be used to distinguish between a data controller and a data processor.

As a starting point, Article 2(d) of the General Directive makes it clear that the relevant criteria for distinguishing between a controller and a processor are whether the party at issue 'determines the purposes and means of processing'. This test only makes sense if it is limited to the particular processing at issue. That is, a party may well process personal data as a data controller for particular purposes (e.g., data of its own employees) and show a considerable degree of autonomy in how its business operations are structured by deciding on the locations of its facilities, developing marketing campaigns, adopting new products and services, etc. However, the only relevant question in establishing whether such a party is a controller or a processor is whether it determines the purposes and means of processing *solely with regard to the particular processing of personal data that is at issue*, not whether it otherwise acts as a data controller or has autonomy in structuring its business operations. It would be impossible for any data processor to function without serving as a data controller for functions such as management of the data of its employees, or without being able to structure its business as it sees fit; any data processing company which did not do so would quickly go out of business.

Nevertheless, the arguments in the DPA opinions show that they have, to a large extent, based their classification of SWIFT as a data controller not on the criteria contained in Article 2(d) of the Directive, but on tasks that any data processor has to perform to conduct its business. Thus, the opinions fail to distinguish between the normal tasks inherent in running a business, and SWIFT's actual role in processing personal data; it is only the latter that is relevant here. For example, data processors in many sectors provide added-value services, and this is not inconsistent with the role of a data processor, as long as it processes personal data solely upon direction of the data controller. Likewise, decisions impacting security (such as the location of SWIFT's operation centers), are crucial to providing a high level of security in SWIFT's operation centers.

Some of the arguments the DPAs made for regarding SWIFT as a data controller seem rather contrived. For instance, classifying SWIFT as a mere data processor should not result in 'splitting' data protection responsibility over too many entities to allow individuals to have meaningful recourse in case of a question or problem. In fact, individuals already have direct relationships with the banks with whom they have accounts and that initiate payment transactions via SWIFT, and it is easier and more effective for them to turn to their banks in case of problems rather than to SWIFT, given SWIFT's reduced ability to provide recourse and its location outside their country.

The real reason why the DPAs decided to regard SWIFT as a data controller seems to be that, as the Article 29 Working Party stated, 'SWIFT decided to comply with the US subpoenas...Indeed, the control mechanisms obtained and operated by SWIFT affected the

¹⁸ Ibid.

purpose and scope of the transfer of data to the UST'.¹⁹ But this is a gross misstatement of the position that SWIFT found itself in when served with the UST subpoenas. Surely neither SWIFT, nor any entity that processes data transferred from the EU, can be deemed to be a data controller merely because it was forced to reveal such data to non-EU law enforcement authorities under mandatory legal process. Indeed, it is ironic that the Article 29 Working Party virtually invited SWIFT to transfer its database from the US to Canada in order to avoid the application of US subpoenas,²⁰ and yet the Canadian Federal Privacy Commission has since found that Canadian data privacy law (which has been recognized as 'adequate' by the EU²¹) does not foreclose SWIFT from responding to a valid subpoena issued in the US.²²

Since mandatory procedures for access to data by law enforcement authorities exist in every country (including in the EU), regarding such access to be incompatible with the status of 'data processor' would mean that there would be no way for a party to ever be a data processor, which would be an absurd result in light of the fact that the General Directive clearly foresees that some entities will be able to act as data processors. It is also wrong to portray the protections obtained under the MOU as a kind of voluntary complicity by SWIFT in the UST access, since non-compliance with a valid subpoena in the US carries severe criminal penalties including fines and imprisonment. Furthermore, any party faced with law enforcement sanctions has a right to defend itself and to attempt to mitigate the measures it is asked to take, and in fact the protections for the data which SWIFT was able to obtain greatly reduced the extent of the UST's access to the data. Had SWIFT refused to comply with the subpoenas, then the UST would have likely seized the entire database and there would have been no protections for the data at all.

¹⁹ Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, November 22, 2006), 11.

²⁰ Ibid, 24, stating 'it is always possible to mirror such a processing outside the EU or EEA in a country that would provide an adequate level of protection. The Working party refers to countries such as Argentina or Canada, that, according to European Commission Decisions, are considered as satisfying the requirements of the Directive...'

²¹ Canadian organisations subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act) have been found by the EU to offer an 'adequate level of data protection'. See Commission Decision (EC) 2002/2 of 20 December 2001 pursuant to Dir (EC) 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act [2002] OJ L2/13.

²² Officer of the Privacy Commissioner of Canada, 'Report of Findings', 2 April 2007, para. 48, available at http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp, stating 'Multi-national organizations must comply with the laws of those jurisdictions in which they operate...[T]o ask the organization to ignore the legitimate laws of other jurisdictions in which they operate is unwise and unworkable...It is for this reason that, in my opinion, the Act acknowledges that an organization that is subject to the Act and that has legitimately moved personal information outside the country for business reasons may be required at times to disclose it to the legitimate authorities of that country. In this case, I am of the view that paragraph 7(3)(c) operates to allow SWIFT to respond to a valid subpoena issued in the United States'.

Thus, while most of the DPA opinions have classified SWIFT as a data controller, they seem to do this almost as an afterthought, and without a detailed examination of the implications of this classification.

Paragraph 2.37

On 1 September 2007, an amendment of the Data Protection Law came into force in Luxembourg which exempts from the Law the processing of personal data of legal entities.

Paragraph 2.72

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.²³ 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.

Paragraph 2.61

On 22 August 2007, a local German court decided that making available on the Internet student evaluations of their teachers was protected by the right to freedom of expression, and did not violate German data protection law, as long as the evaluations did not contain false information or defamatory comments.²⁴

Paragraph 2.80

In two decisions,²⁵ the Paris Court of Appeal ruled in 2007 that the IP address used by an internet user does not constitute personal data, because it does not allow the user's direct or indirect identification. Both decisions relate to a piracy case, in which the French Société civile de producteurs de phonogrammes (SCPP) had lodged a complaint against an unidentified individual for using software enabling him to download and share illegally hundreds of music files. One of the SCPP's anti-piracy agents monitoring the network had collected the pirate's IP addresses and sent them to the police for investigation. However, the French Data

²³ See also Appendix 13.

²⁴ Landgericht Köln, Beschluss vom 22. August 2007, no 28 0 333/07 (2007) *Recht der Datenverarbeitung* 252.

²⁵ Cour d'appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007, available at http://www.legalis.net/jurisprudence-decision.php3?id_article=1954; and Cour d'appel de Paris 13ème chambre, section A Arrêt du 15 mai 2007, available at http://www.legalis.net/jurisprudence-decision.php3?id_article=1955.

Protection Authority (CNIL) has expressed disagreement with the two decisions,²⁶ and they are currently being appealed, so that the status of IP addresses is unclear in France.

On 8 August 2007, the Swedish Court of Appeal held that the processing of IP addresses by the Swedish anti-piracy organization constitutes the processing of personal data.²⁷ The judgment confirms the decision by the Swedish Data Protection Authority from 2005 that any processing of IP numbers by the anti-piracy organization will continue to be subject to data protection rules. The anti-piracy organization works to protect copyrighted work from piracy, in particular by collecting IP numbers for the purpose of tracing persons distributing copyright materials online, and uses the data to make police-reports and to notify internet service providers of breaches of internet subscription rules.

Paragraph 2.83

On June 20 2007, the Article 29 Working Party adopted Opinion 4/2007 on the definition of personal data.²⁸ The opinion analyzes each of the four elements of the definition of personal data, i.e., ‘any information’, ‘relating to’, ‘an identified or identifiable’, and ‘natural person’, with supporting examples taken from the practice of national DPAs.

In *Case of Copland v. The United Kingdom*,²⁹ the European Court of Human Rights found that the e-mail and Internet usage of the employee of a public body were protected under Article 8 of the European Convention of Human Rights.

Paragraph 2.86

The fact that data may not be considered ‘personal data’ within the scope of the General Directive does not mean that there are no legal restrictions on their processing.³⁰ First of all, the rules of instruments such as the European Convention on Human Rights may still apply to the data, notwithstanding the fact that they are not covered by EU law. In addition, other types of law such as tort law and criminal law may also apply to data that are not considered ‘personal data’ within the scope of data protection law.

Paragraph 2.94

²⁶ See CNIL press release of 2 August 2007, available at <http://www.cnil.fr/index.php?id=2244&news%5buid%5d=484&cHash=f2a66a27ee>.

²⁷ See press release is available (in Swedish) at <http://www.datainspektionen.se/nyhetsarkiv/nyheter/2007/Juni/2007-06-20.shtml>.

²⁸ Article 29 Working Party, ‘Opinion 4/2007 on the concept of personal data’ (WP 136, 20 June 2007).

²⁹ Application no. 62617/00 (3 April 2007) ECHR.

³⁰ See Article 29 Working Party, ‘Opinion 4/2007 on the concept of personal data’ (WP 136, 20 June 2007) 24.

In one case, the Austrian Data Protection Commission refused to allow a company to collect information regarding the relationship of emergency contact persons to the employees who had indicated them, since this could reveal that the contact person and the employee were in a homosexual relationship.³¹

³¹ Datenschutzkommission [Austria], Bescheid internationaler Datenverkehr, no. K.178.215/0008-DSK/2006, 20 October 2006.

Chapter 4

Paragraph 4.28

State DPAs in Germany have questioned the legal sufficiency of the standard contractual clauses. German data protection law implements a two-step approach for use of the clauses: in the first step, an assessment is made of whether or not there is a legal basis for processing personal data under German data protection law, in particular under § 4 or § 28 of the German Federal Data Protection Act. The use of standard contractual clauses may then be considered in a second step in order to assess whether or not ‘adequate safeguards’ are ensured according to § 4b and § 4c para. 2 of the Act (which implement Articles 25 and 26 of Directive 95/46/EC).

In a paper adopted by the *Arbeitsgruppe ‘Internationaler Datenverkehr’* of the group of German data protection authorities (a subgroup meeting on international data transfers of the conference of German federal and state data protection authorities or *Düsseldorfer Kreis*) on 12-13 February 2007, it is stated that the alternative standard contractual clauses of 2004 are not suitable for the transfer of employee data and may need to be expanded by additional clauses, since the liability and informational obligations are ‘limited’.¹ This follows a paper dated 6 June 2006 prepared by the DPA of the federal state of Hessen in preparation for a meeting in Berlin of the *Arbeitsgruppe* which raises various questions about the adequacy of the alternative standard contractual clauses. In particular, questions are raised about the lack of joint and several liability (Clause III.a), the provision concerning the data importer’s duty to give information about processing to data subjects (Clause I.d), and the assertion of rights primarily against the data importer (Clause II.b) (see pages 4-5). The paper asks if these provisions are ‘acceptable’ (‘Sind diese Regelungen...akzeptabel?’). The paper then goes on to question the adequacy of Clause II.d, and para. 7 of Annex A.

The General Directive does not give a clear indication of the boundary between the two steps of the legal analysis that must be undertaken when determining the legality of an international data transfer. However, such a boundary can be defined by examining the purpose of the two steps. The purpose of step one is to ensure that the initial processing of personal data is legal under applicable national law, whereas the purpose of step two is to ensure that adequate protection or adequate safeguards will apply to processing of the data once they have been transferred outside the EU. Thus, for example, it is entirely legitimate for national law to require the conclusion of an agreement with the works council before employee data can be transferred under the standard clauses, since this requirement may derive from national employment law and is often required even for transfers of personal data within the EU, i.e., it is not directed solely at ensuring an ‘adequate level of protection’ for data transfers outside the EU. However, any criticism of the level of protection of specific provisions of the standard contractual clauses must be found to involve step two, since the clauses are designed to provide adequate safeguards for the international transfer of personal data.²

¹ Abgestimmte Positionen der Aufsichtsbehörden in der AG ‘Internationaler Datenverkehr’ am 12./13. Februar 2007, p. 2.

² See Article 26(2) of Directive 95/46/EC.

The German DPAs are in effect attempting to ‘repackage’ concerns that actually relate to the level of protection under step two as falling within their discretion to ensure that there is a legal basis for processing under step one; for example, in the minutes of the Berlin meeting referred to above, it is stated that ‘in examining the first step (‘protectable interest of the data subject’) data export agreements which are insufficient under German law may be taken into account’.³ The criticisms they make about the standard clauses clearly concern the substance of the protections included in them, rather than the initial legality of processing, and thus fall within step two, which has been settled once and for all by the Commission decisions.⁴ For example, any criticism that the alternative clauses results in a ‘lowering of the level of data protection’ (*Absenkung des Datenschutzniveaus*) as in the article by the Berlin DPA quoted above is clearly calling into question the Commission decision approving the clauses as offering ‘adequate protection’. While the DPAs state in the minutes of the Berlin meeting that ‘the first step (material permissibility under national law) may not be evaded by signature of the alternative standard contractual clauses in the second step’,⁵ the reverse is also true: the legal effect of the Commission’s decisions approving the standard contractual clauses as providing ‘adequate protection’ may not be evaded by deeming questions related to the adequacy of protection (step two) to fall within the DPAs’ discretion to determine compliance with national law (step one). While the DPAs do have the discretion under national law to determine the conditions for satisfying step one, such discretion is not unlimited, and must be subordinate to conflicting rules under EU law.

Under Article 249 para. 4 of the EC Treaty, any Commission decision is binding upon those to whom it is addressed, and the Commission decisions on the standard contractual clauses are addressed to the Member States (see Article 7 of the 1001/497 Decision, and Article 3 of Decision 2004/915). A decision which has been addressed to all Member States constitutes a legislative act,⁶ and is binding on all institutions of the Member State concerned, including the judiciary. Accordingly, Member States are under a duty by virtue of the primacy of Community law to refrain from applying any national provisions which would be likely to hinder the implementation of a Commission decision.⁷

Based on case law concerning the correct implementation of directives, national authorities are under a duty to refrain from applying national provisions which conflict with the

³ Page 5: ‘Bei der Prüfung der 1. Stufe (‘schutzwürdige Interessen des Betroffenen’) können (nach deutschem Recht unzureichende) Vereinbarungen über den Datenexport bereits berücksichtigt werden’.

⁴ See P Gola and C Klug, ‘Die Entwicklung des Datenschutzrechts in den Jahren 2006/2007’ (2007) *Neue Juristische Wochenschrift* 2452, 2458.

⁵ Page 6: ‘Die 1. Stufe (materielle Zulässigkeit nach nationalem Recht/BDSG) könne nicht durch den Abschluss der (Alt.) StV auf der 2. Stufe umgegangen werden’.

⁶ See, e.g. Council Decision 98/415/EC of 29 June 1998 on the consultation of the European Central Bank by the national authorities on draft legislative provisions, [1998] O.J. L 189/42. Regarding decisions addressed to the Member States, see Mager, ‘Die staatengerichtete Entscheidung als supranationale Handlungsform’ (2001) *EuR* 661-681.

⁷ ECJ, Case 249/85 *Albako* [1987] E.C.R. 2345, para. 17.

provisions of a directive.⁸ Moreover, all the authorities of a Member State must take, according to their respective powers, all the general and particular measures necessary to ensure that the result sought by the Directive in question is achieved.⁹ In this case, the result sought by a Commission decision under Article 26(4) of Directive 95/46/EC is to provide a standardized way of transferring personal data outside the EU, and this result is frustrated if a Member State DPA regards the adequacy of a data transfer method standardized by a Commission decision as falling within its national competence.

Apart from the substantive data protection issues involved, the way that the German DPAs are raising these issues holds the potential to severely damage the utility of the standard contractual clauses. If the DPAs believe that the clauses do not offer ‘adequate safeguards’, then the correct course of action is for them to discuss this issue within the Article 29 Working Party and have the Working Party attempt to convince the Commission to modify its decision, rather than each national or local DPA taking unilateral action on a national level. If each DPA were to take similar action on its own, then there would soon be at least 27 different sets of additional national requirements to be fulfilled when using the standard contractual clauses, and they would become useless. In fact, this multiplicity of national requirements for approval of contractual clauses, which was the case before the standard clauses were approved, was precisely the situation that the standard contractual clauses were supposed to remedy.

This is not just a German issue: if other Member State DPAs raise additional challenges to the adequacy of the alternative standard contractual clauses, then this will effectively make the Commission decisions approving them useless.

Paragraph 4.48

On 9 October 2007, the Article 29 Working Party assessed the adequacy of data protection law in Jersey¹⁰ and in the Faroe Islands.¹¹ With respect to the Faroe Islands, the Article 29 Working Party determined that, except for a missing provision regarding automated individual decisions, the Faroese law complies with most of the EU data protection principles. Taking the view that adequacy does not mean complete equivalence with the level of protection set by the Data Protection Directive, the Working Party concluded that the Faroe Islands ensure an adequate level of protection within the meaning of Article 25(6) of the General Directive. Regarding Jersey, the law of which is an embodiment of UK law, the Article 29 Working Party found that a number of provisions differ substantially from the Directive, in particular the definition of personal data, unnecessary restrictions to the transparency principle, or the powers of the Data Protection Commissioner. The Working Party considered however that these differences were not significant in relation to the

⁸ ECJ, Case 103/88 Fratelli Costanzo [1989] E.C.R. 1839, para. 33.

⁹ ECJ, Case C-72/95 Kraaijeveld [1996] E.C.R. I-5403, para. 61; ECJ, Case C-435/97 World Wildlife Fund [1999] E.C.R. I-5613, para. 70.

¹⁰ Article 29 Working Party, ‘Opinion 8/2007 on the level of protection of personal data in Jersey’ (WP 141, 9 October 2007).

¹¹ Article 29 Working Party, ‘Opinion 9/2007 on the level of protection of personal data in the Faroe Islands’ (WP 142, 9 October 2007).

protection provided for personal data transferred from EU Member States to Jersey, and concluded that Jersey ensures an adequate level of protection within the meaning of Article 25(6).

Paragraph 4.61

A company's safe harbor certification is valid for one year from the date that it is entered into the safe harbor list by the US Department of Commerce.

Safe harbor membership by data processors

One of the most vexing questions which often arises in practice is what implications safe harbor membership holds for a company that considers itself to be a 'data processor'. In many cases, a company may act as a data controller with regard to certain functions of data processing, and as a processor with regard to other functions, and it can be difficult to distinguish the two sets of functions.

It may be asked whether much importance should be granted to the distinction between data controller and data processor in the safe harbor context, since the safe harbor principles state that any interpretation of them is to be based on US law,¹² which knows no such distinction. However, the safe harbor principles must be interpreted against the backdrop of the EU legal framework for international data transfers, since it was that framework which led to the enactment of the safe harbor in the first place. Indeed, if there is evidence that a safe harbor member company is violating the principles or any safe harbor enforcement body is not effectively fulfilling its role, then the European data protection authorities and the European Commission may take variety of actions ranging from suspension of data flows to the member company, to reversal or suspension of the safe harbor adequacy decision,¹³ which actions would remove any incentive for companies to join the safe harbor scheme in the first place. The best view is that, while the safe harbor itself is an instrument of US law, it is informed by EU data protection concepts, and was drafted as a response to those concepts in order to provide a legal basis for data transfers to the US. Thus, while the basis for interpretation of safe harbor should be US law, such interpretation should be informed by relevant concepts of EU data protection law where appropriate. Interpretation of safe harbor thus involves a balancing act between US and EU legal concepts in which both sets of concepts should be considered, but neither is given complete dominance over the other.

The importance of the distinction between a data controller and a data processor in the safe harbor context arises because of the obligations that are put on a company when it joins the safe harbor. Upon membership of the safe harbor, a company is in effect pledging to the world that it complies with the safe harbor principles in processing personal data (called 'personal information' in the safe harbor documents); if it does not so comply, then it may be

¹² See Safe Harbor principles, stating 'US law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by Safe Harbor organisations, except where organisations have committed to cooperate with European Data Protection Authorities'.

¹³ Safe Harbor Decision, Article 3.

liable under the US Federal Trade Commission (FTC) Act.¹⁴ Thus, the ability to comply with the safe harbor principles is of critical importance so that the safe harbor member company may avoid legal liability.

The safe harbor principles themselves do not use the terms ‘data controller’ or ‘data processor’. The safe harbor decision of the European Commission and related documents refer instead to the concept of ‘organization’, which term sometimes seems to be used in a colloquial sense as any entity processing personal data (whether data controller or data processor)¹⁵ and other times more specifically in the sense of ‘data controller’¹⁶, and to the concept of ‘agent’, which seems to be used in the sense of data processor.¹⁷

The lack of clarity in the safe harbor documents regarding terms such as ‘organization’ and ‘agent’ can create doubt for a company that is seeking to join the safe harbor and is unsure whether it would be considered a data controller or a data processor. To give an example, the safe harbor access principle provides that ‘individuals must have access to information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated’. A legal duty to provide access for data protection purposes generally does not exist under US law, so it is difficult to use US law to interpret this principle. Under EU data protection law, access should only be granted by a data controller, and not by a data processor, so that this principle would seem to apply only to safe harbor members that are data controllers. However, a company joining safe harbor which considers itself a data processor would understandably be reluctant to conclude that the Principle is not applicable to it, since it may be liable under the FTC Act if it is wrong. Thus, potential safe harbor member companies which believe that they may be data processors need to evaluate the status of data processors under the safe harbor system, and their potential for complying with the safe harbor principles, in order to minimize compliance risks and ensure that they can comply with the safe harbor framework.

¹⁴ See safe harbor principles, stating ‘Where in complying with the Principles, an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.’

¹⁵ See, e.g., the Safe Harbor Decision, Recital 5, providing that ‘The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if *organisations* comply with the Safe Harbor Privacy Principles for the protection of personal data transferred from a Member State to the United States and the Frequently Asked Questions providing guidance for the implementation of the Principles issued by the Government of the United States on 21.07.2000’ [emphasis added].

¹⁶ E.g., providing access to personal data under the Access Principle, which provides that ‘individuals must have access to personal information about them that an *organization* holds...’ [emphasis added]. See Article 12 of the General Directive, which provides that access is a right to be exercised against the data controller.

¹⁷ E.g., in the Safe Harbor Choice Principle, footnote 1 of which refers to an agent as a third party that performs ‘task(s) on behalf of and under the instructions of the organization’.

Safe harbor FAQ 10 raises a question in this regard, since it seems to state that safe harbor member companies who are data processors do not need to comply with most of the safe harbor principles, and in effect only need to comply with the requirement to have in place a data processing contract between the US organization participating in the safe harbor and the data controller in the EU.¹⁸ However, it is risky for a safe harbor member company to rely on this language to avoid complying with the rest of the safe harbor principles, for several reasons. As explained above, it can be difficult for a company to state with confidence that it is only a data processor, and not also a data controller. Thus, a company joining the safe harbor and not implementing the safe harbor principles beyond the requirement to have a data processing agreement in place with a European data exporter will be taking the risk that in case of a dispute it would be found to be a data controller. Moreover, many safe harbor member companies that refer to themselves as data processors have implemented most if not all of the other safe harbor principles. It has thus become best practice for data processors joining the safe harbor also to comply with the other safe harbor principles as outlined below, notwithstanding FAQ 10. Such compliance should not prejudice the status of a safe harbor member company as a data processor.

Questions are sometimes raised as to whether a data processor may join the safe harbor, but in fact there is no reason why a company acting as a data processor or agent should not be allowed to join. Several considerations argue in favor of allowing data processors to join safe harbor:

- As explained above, there is considerable uncertainty under European data protection law regarding the distinction between a data controller and a data processor. In view of this, restricting safe harbor membership to companies that are clearly data controllers would greatly restrict the number of companies that could join.
- The safe harbor principles and supporting documentation do not indicate any intent of the US or the EU to restrict safe harbor membership to data controllers. In fact, safe harbor FAQ 10 asks ‘When data is transferred from the EU to the United States only for processing purposes, will a contract be required regardless of participation by the processor in the safe harbor?’, which clearly contemplates that data processors may join.
- Since safe harbor must be interpreted under both US law and EU law, restricting membership solely to data controllers as the term is interpreted under EU law would seem inappropriate.
- The US Department of Commerce ultimately approves the safe harbor applications of companies and enters them on the list of safe harbor members, and the safe harbor list includes a number of companies that describe themselves as data processors.¹⁹ This indicates that, over the eight years that the safe harbor has been in existence, the

¹⁸ FAQ 10, stating in part: ‘A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it *vis-à-vis* the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles)’.

¹⁹ For example, the Safe Harbor member companies Acxiom; Database Marketing Technologies, Inc.; Davis Direct WorldWide; Global DM Solutions, Inc.; and Phoenix data Processing, LLC.

Department of Commerce accepts the notion that data processors may join the safe harbor, and that a kind of customary law has crystallized in this regard. Moreover, the safe harbor application process itself does not require a company to state whether it is a data controller or a data processor, indicating that this distinction is not relevant in determining whether a company may join safe harbor.

Joining safe harbor requires more thought for a company that considers itself a data processor than it does for a company that considers itself a data controller. This is because, first of all, the company will have to decide how it describes itself in the relevant safe harbor documents, and secondly, because the policies and procedures it adopts to implement the safe harbor principles need to be tailored to its status as a data processor.

The company should carefully consider how it describes itself in its policies and procedures, in order not to contradict statements it may have made in other contexts. For example, if a company has notified data processing to the European data protection authorities (DPAs) covering the processing of data that will be transferred to the US under safe harbor, it may be difficult to justify considering itself a data processor for safe harbor purposes, since notification to the DPA is something that is typically done by a data controller. It is also important to be realistic about whether a company is in fact merely a data processor, or whether it could also be considered a data controller. A company seeking to join safe harbor should be realistic in its characterization, and not call itself a data processor if it would not be able to argue this with a straight face to a data protection authority. On the other hand, if a company is truly convinced that it is only a data processor, then there is no reason not to make this clear in its policies and safe harbor registration.

It is possible for a company to be a data processor with regard to one type of processing and a data controller with regard to another type of processing, so that if the company believes strongly that it is only a data processor for certain types of data transfers and processing in the US, it should clearly differentiate such processing in its safe harbor policies from any other types of processing for which it may be a data controller, in order to avoid confusion. This possibility gives companies many options to characterize their data processing and structure their safe harbor policies, so that they may characterize themselves as data processors only for those types of processing for which this characterization truly fits.

A company should also carefully examine the safe harbor principles to determine how it will satisfy them as a data processor. In some national data protection regimes, it is not uncommon for data controllers and data processors to cooperate so that the processor may in effect outsource compliance with certain obligations of data protection law to the data controller. A number of safe harbor policies that have been accepted by the Department of Commerce provide for procedures under which the safe harbor member who is a data processor may structure its compliance obligations so that they are fulfilled by cooperating with the data controller. The following are excerpts from two such policies:

- Safe harbor policy of the company Global Village Marketing & Data Services, Inc: 'GVM acts as a Data Processor (an entity that processes data on behalf of a data controller) and therefore processes data in accordance with the instructions of the Data Controller (an entity that determines the purposes and means for processing personal data). As a Data Processor, GVM shall not transfer data to a Third Party (any entity other than the Data Processor or the Data Controller) without instructions from the Data Controller. GVM will process the data for one-time use and only for the purpose for which it was intended. Written Instructions shall be provided by the Data Controller

outlining the authority granted to GVM as the Data Processor, and specifying in the instructions, the limits of that processing so that GVM may keep on record our classification as a Data Processor. Without written instructions, GVM will not be liable for the actions of the Data Controller.²⁰

- Safe harbor policy of the company Global DM Solutions: 'Global DM Solutions abides by the safe harbor principles developed by the US Department of Commerce and the European Commission. It receives personal data transferred from the EU to the US merely as a Data Processor on behalf of Global DM Solutions' clients. In this capacity, Global DM Solutions acts as the Data Processor and Global DM Solutions' clients act as the Data Controller. Global DM Solutions does not own or control any of the information it processes on behalf of Global DM Solutions' clients. All such information is owned and controlled by Global DM Solutions' clients. Processes performed by Global DM Solutions on behalf of its clients are pursuant to the instructions of the applicable client. Global DM Solutions may use the services of third party Data Processors to process personal data in accordance with purposes identified for such personal data by the applicable client...Clients of Global DM Solutions may obtain copies of personal data maintained on its customers or request that personal data about its customers be corrected, amended or deleted by submitting their request in writing to Global DM Solutions. In an effort to protect the privacy of data subjects, Global DM Solutions will not provide a data subject with access to his or her personal data without the written instructions of the applicable Global DM Solutions client.'²¹

These are just two examples of companies which have joined the safe harbor and have been able successfully to structure their compliance obligations while maintaining their status as data processors.

The data processor joining safe harbor should have a privacy policy which explains how it implements the safe harbor principles in its data processing practices. In a typical situation involving a safe harbor registration by a data processor, the company may have no direct contact with the individuals or companies whose personal data are being processed, and it is the data controller who engages the data processor to process data on its behalf (often the client or subsidiary of the safe harbor member company) that has such relationships. For example, if the safe harbor member provides outsourcing services to a data controller in the EU, then it will typically not have any contact with the individuals whose data the data controller is transferring to it for processing, and will be under strict constraints based on data protection law, confidentiality obligations, and contractual commitments which prevent it from contacting such individuals or processing their personal data beyond the directions given by the data controller. In such a situation, the only way for the data processor to comply with the safe harbor principles is to indicate in its safe harbor policy that it is cooperating with the original data controller to comply with the principles. This can require careful consideration by the data processor seeking to join safe harbor, since it will require the data processor to take actions such as indicating to the original data controller that it should give notice to the individuals whose personal data are being processed that they have a right to opt-out of their data being disclosed to third parties (the data controller is generally required to take such action anyway under the national data protection law to which it is subject). It is important for the data processor merely to indicate that it has informed the

²⁰ Available at <http://www.globalvillagemktg.com/legal/safeharbor.php>.

²¹ Available at http://www.globaldmsolutions.com/privacy.html#safe_harbor.

original data controller that it should take such actions, and not to warrant that the data controller has actually done so, so that it does not assume any liability should the data controller fail to do so. Ideally these steps should be memorialized in an agreement between the data processor and data controller.

In drafting the policy, compliance with the safe harbor principles should be explained in a positive sense rather than a negative sense. That is, rather than stating that the member company cannot comply with a certain Principle by itself because it is not a data controller and does not have a direct relationship with the individual whose data it is processing, the company should indicate how compliance is based on cooperation between the company and the original data controller. It is advisable to avoid using the terms 'data controller' and 'data processor' in the policy unless there is a specific reason to do so, in order to avoid introducing EU legal terms into the policy (in the formulations below, the safe harbor member company is referred to as an 'agent').

The following explains how each of the safe harbor principles may be complied with in a case involving a data processor that does not have a direct relationship with the data subjects whose personal data it is processing; for each Principle, language is proposed that a company could use in its safe harbor policy. It is important to remember that drafting a safe harbor privacy policy requires an investigation of the member company's data processing practices, to ensure that it can comply with the safe harbor principles. Thus, this language is just exemplary, and must be tailored to a company's specific situation before being used.

Notice Principle: Data subjects have to be informed about the collection of data and the purposes of such collection, how to contact the safe harbor member organization to inquire or complain, the types of third parties to which it discloses data, and the choices and means to limit their use and disclosure. This information should be given in the safe harbor policy, which should be available on the company's web site (except in the case of registrations for human resources data, for which the privacy policy may be placed on the company's internal Intranet instead). Here is possible language for the safe harbor policy:

As an agent processing personal information under the direction of its customers, XYZ COMPANY has no direct relationship with the individuals whose personal data it processes. XYZ COMPANY works with its customers to help them provide notice of data processing to individuals, including information concerning (1) the purposes for which personal information is collected and used; (2) a contact person to whom enquiries or complaints may be directed; (3) the types of third parties to whom personal information is disclosed; and (4) the choices and means that individuals are offered for limiting use and disclosure of personal information.

Choice Principle: Individuals must be provided with the possibility of opting out of disclosure of their personal data to a third party and of their use for purposes other than those for which they were collected. However, it is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures. Opt-in consent must be obtained for the processing of 'sensitive data' (meaning personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual). The safe harbor member company must thus determine whether companies to which personal data will be disclosed are data

controllers or data processors, in order to determine whether or not individuals should be given a chance to opt-out of such disclosure. The data processor should agree on a procedure with the original data controller whereby the controller informs the processor about the purposes for which the personal data were originally collected and whether any individual has opted-out of disclosure to any third parties, and the processor should implement the individual's choice in such cases. Here is possible language for the safe harbor policy:

As an agent processing personal information under the direction of its customers, XYZ COMPANY has no direct relationship with the individuals whose personal data it processes. XYZ COMPANY may disclose personal data to third parties in the following instances: [INSERT DETAILS]. XYZ COMPANY works with its customers to help them inform individuals about the possibility of such disclosures and provide individuals with the choice of opting-out of them. XYZ COMPANY only processes personal information for purposes that are compatible with those for which it was originally collected or subsequently authorized by the individual. [Statement that XYZ COMPANY does or does not process any sensitive data, and an explanation of how opt-in consent is provided for the processing of any such data.]

Onward transfer Principle: The safe harbor member company seeking to transfer personal data to another company or entity that has not subscribed to the safe harbor principles must ensure that the safe harbor notice and choice principles have been complied with regarding the onward transfer. However, if the third party is an agent, then the company must either ascertain that the third party subscribes to the safe harbor principles or is subject to EU data protection law or another EU adequacy finding, or it must enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the safe harbor principles. The safe harbor member company must thus determine whether companies to which personal data will be transferred are data controllers or data processors, to determine what steps should be taken. Here is possible language for the safe harbor policy:

Personal information may be transferred to [insert information about data controllers] and [insert information about data processors]. Transfers to [insert information about data controllers] are covered by the provisions in this Policy regarding notice and choice. XYZ COMPANY has concluded agreements with [insert information about data processors] requiring that they provide at least the same level of privacy protection as do the safe harbor principles.

Any company processing personal data in the US is subject to US law, which includes an obligation to cooperate with lawful requests for access to data by law enforcement authorities. It may thus be advisable for the company to include some language about the possibility of law enforcement access to personal data in its safe harbor policy. The safe harbor framework contains exceptions to adherence to the principles for the purpose of

meeting law enforcement requirements;²² however, the scope of these exceptions, and their legal effect, is controversial. There are two possible strategies that can be followed here, namely either to rely on the exceptions in the safe harbor for law enforcement access to data (i.e., in effect to categorize law enforcement access as falling outside the safe harbor framework), or to explain the possibility of law enforcement access as a kind of onward transfer under the safe harbor framework. Possible language for the first approach (relying on the law enforcement exception in safe harbor) could be the following:

As set out in the US safe harbor principles, adherence to the principles may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements.

Possible language for the second approach could read as follows:

Please be aware that in certain circumstances, it is possible that personal information may be subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders.

Security Principle: A safe harbor member company must take reasonable precautions to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction. Transfers to the US for the purpose of ‘mere processing’ additionally require the EU-based controller and the US-based processor to enter into a data processing agreement (an ‘Article 17 contract’ under that article of the General Directive) to protect the controller’s rights under EU law; such contracts must also be concluded between the US data importer and any third parties to whom it outsources processing.²³ Here is possible language for the safe harbor policy:

XYZ COMPANY offers a high level of data security to protect message data from loss, misuse and unauthorized access, disclosure, alteration and destruction. As an agent processing personal information under the direction of its customers, XYZ COMPANY has concluded a contract with its customers specifying the conditions under which personal information received from the EU are processed and kept secure. XYZ COMPANY has appropriate contractual language in place with third party data processors providing that they must apply the safe harbor principles to the processing of personal data received from XYZ COMPANY.

²² See the safe harbor principles, which provide ‘Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization....Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis...’

²³ See Appendix 9 for an example of an Article 17 contract.

Data integrity Principle: The personal data processed must be relevant for the purposes for which they are to be used. Furthermore, personal data may not be processed in a way that is incompatible with the purposes for which they have been collected or subsequently authorized by the data subject. Reasonable steps must be taken to ensure that data are reliable for their intended use, and that the data are accurate, complete, and current. Here is possible language for the safe harbor policy:

XYZ COMPANY only processes personal data that are relevant to the services it provides, and only for purposes compatible with those for which the data were collected. As an agent processing personal information under the direction of its customers, XYZ COMPANY works with its customers so that they can provide a way for individuals to correct their data.

Access Principle: Individuals must have access to all personal data processed by the safe harbor member company, and must be able to correct, amend or delete inaccurate data. The right of access is limited by the principle of reasonableness, and companies may charge a fee to provide access and can limit the number of access requests within a given period. Here is possible language for the safe harbor policy:

As a data processor, XYZ COMPANY has no direct relationship with the individuals whose personal data it processes. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct his query to the client of XYZ COMPANY (the data controller) which has transferred such data to the XYZ COMPANY for processing. The client will then provide access to the individual as determined under the applicable local data protection law.

Enforcement Principle: The safe harbor member company must provide recourse for individuals by joining a self-regulatory privacy program that includes an alternative dispute resolution mechanism, or by agreeing to cooperate with EU DPAs. The wording of a safe harbor policy with regard to enforcement need not be any different for a data processor joining safe harbor than it would be for a data controller.

Paragraph 4.66

On 6 June 2007, the European Commission rejected a complaint that the transfer of personal data about employees of the Greek subsidiary of a US multinational company, Abbott Laboratories, violated the data protection rights of its employees. The issue was raised by a Greek member of the European Parliament in connection with a letter sent by the Greek subsidiary of Abbott Laboratories to its employees informing them about the collection, processing and transfer of sensitive personal data to companies in the Abbott Group and to the United States or to government authorities. In its response, the Commission emphasized that transfers of personal data to a company in the United States that adheres to the safe harbor scheme are not in breach of the General Directive.²⁴

²⁴ European Parliament, Question no 36 by Anthansios Pafilis, Subject: Recording and forwarding of personal data by US company, available at <http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20070524&secondRef=ANN-01&language=EN&detail=H-2007-0326&query=QUESTION>.

Paragraph 4.98

On March 21 2007, the Austrian Data Protection Commission (DSK) rejected an application for a data transfer from an Austrian subsidiary to its US parent company, and found the purpose mentioned in the annexes to model contract submitted for approval ('for worldwide statistic reports and editing') to be invalid. The applicant explained to the DSK that no editing would be taking place in the US. The DSK, however, found that this explanation was unsatisfactory, since the contractual basis for transfer of the data to the US would allow the data importer a considerably broader use of the data than what was initially requested by the data exporter. Therefore, an approval which restricts the data processing abroad would be difficult to enforce. Further, the DSK pointed out that considering the special organizational structure of a holding, the enforcement of law by the Austrian exporter against the US data importer would realistically not be successful, since the data importer as the superior parent entity has decisional powers over the Austrian entity. Finally, the DSK considered the transfer to be serious because of the comprehensiveness of HR data that was supposed to be transferred as well as the potential of breach.²⁵

Paragraph 4.109

In its opinion in the SWIFT affair, the Article 29 Working Party found that the transfer of personal data in the SWIFT database could not be justified under Article 26(1)(b) of the General Directive as being necessary for the performance of a contract between the data controller and a third party, without explaining in detail why this was so.²⁶

Paragraph 4.115

In its opinion in the SWIFT affair, the Article 29 Working Party found that the transfer of personal data in the SWIFT database could not be justified under Article 26(1)(d) of the General Directive as being necessary or required on important public interest grounds, or for the establishment, exercise or defence of legal claims, since the SWIFT database could have been located in a country that had been found to offer an 'adequate level of data protection' (such as Argentina or Canada) rather than in the US, and the public interest involved was not that of an EU Member State.²⁷

Paragraph 4.124

²⁵ Datenschutzkommission, Bescheid internationaler Datenverkehr, no GZ: K178.231/007-DSK/2007, 21 March 2007, available at <http://www.ris.bka.gv.at>.

²⁶ Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, 22 November 2006) 24.

²⁷ Ibid.

Germany: On 1 June 2007, the DPA of the German federal state of Hessen approved the BCRs of Merck.²⁸ The BCRs are wide-ranging and cover data of employees, business partners, customers, and suppliers, as well as clinical trial data.

UK: On 9 May 2007, the UK Information Commissioner approved the BCRs of Philips, which cover both employee and customer data.²⁹

Paragraph 4.127

On 10 January 2007, the Article 29 Working Party adopted a recommendation for a standard application for approval of BCRs, which is based heavily on the ICC submission and adopts the majority of its text verbatim, with some important additions and deletions.³⁰

²⁸ See the DPA's press release of 12 June 2007 (in German only) at http://www.rp-darmstadt.hessen.de/irj/RPDA_Internet?rid=HMdI_15/RPDA_Internet/nav/1e3/1e3605fe-78c2-9011-1010-43765bee5c94,ec40fe7f-dad1-311d-5ce7-b44e9169fccd,,,11111111-2222-3333-4444-100000005002%26_ic_uCon=ec40fe7f-dad1-311d-5ce7-b44e9169fccd%26shownav=false.htm&uid=1e3605fe-78c2-9011-1010-43765bee5c94&shownav=false.

²⁹ See the Information Commissioner's press release at http://www.ico.gov.uk/upload/documents/pressreleases/2007/philips_authorized_by_ico_to_transfer_personal_information....pdf.

³⁰ Article 29 Working Party, 'Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data' (WP 133, 10 January 2007).

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 application of the different legal bases (consent, employment contract, legitimate interest, collective agreement) and concludes that

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>.

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

Paragraph 5.93

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.’

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

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/informationmaterial/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.

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.

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

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

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.

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.

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 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.

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

- 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 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

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.

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

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.

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

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

‘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.

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</p> <p><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[uid]=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: php?id=2225&f=ebdcfcbe</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/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf</p>

	<p>17 December 2007 <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 <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>

Appendix 14

Documents Adopted by Article 29 Working Party (from September 2006-) UPDATED APRIL 2008

Reference	Date	Document
WP 124	27.09.2006	Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement
WP 125	26.09.2006	Working document on data protection and privacy implications in eCall initiative
WP 126	26.09.2006	Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive
WP 127	27.09.2006	Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data
	29.09.2006	Whistleblowing: Letter addressed on 29 September 2006 to the Chairman of the Working Party by the Director of the Office of International Affairs of the Securities and Exchange Commission (SEC)
WP 128	22.11.2006	Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)
WP 129	09.01.2007	Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities
WP 130	24.01.2007	1st European Data Protection Day
WP 131	15.02.2007	Working Document on the processing of personal data relating to health in electronic health records (EHR)
WP 132	15.02.2007	Annex: Short notice for travel between the European Union and the United States
	15.02.2007	Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities
WP 133	10.01.2007	Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data
WP 134	01.03.2007	Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications

		(COM(2006)269 final
WP 135	15.02.2007	Revised and Updated Policy to promote the transparency of the activities of the Working Party established by Article 29 of Directive 95/46/EC
WP 136	20.06.2007	Opinion N° 4/2007 on the concept of personal data
WP 137	20.06.2007	Report 1/2007 on the first joint enforcement action: evaluation and future steps
WP 138	17.08.2007	Opinion N° 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007
WP 139	20.09.2007	Opinion 6/2007 on data protection issues related to the Consumer Protection Cooperation System (CPCS)
WP 140	20.09.2007	Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)
WP 141	09.10.2007	Opinion 8/2007 on the level of protection of personal data in Jersey
WP 142	09.10.2007	Opinion 9/2007 on the level of protection of personal data in the Faroe Islands
WP 143	23.11.2007	8th Directive on Statutory Audits, Opinion 10/2007 by the Article 29 Working Party
WP 144	05.12.2007	2nd Data Protection Day
WP 145	05.12.2007	Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007
WP 146	18.02.2008	Work Programme 2008-2009, Article 29 Working Party
WP 147	18.02.2008	Working Document on the protection of Children's Personal Data

Appendix 15

On 10 January 2007, the Article 29 Working Party approved the ICC standard application form for BCRs (reproduced in this Appendix), with some modifications (see updated para 4.127 below). The approved version of the form can be found at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp133_en.doc