

Christopher Kuner

European Data Protection Law

Oxford University Press

Internet Update 1.0/September 2007

Chapter 1

Paragraph 1.07

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

Paragraph 1.25

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

Paragraph 1.33

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

One commentator has noted that ‘funding for enforcement of the European Union’s complex and stringent data protection law varies widely within the 27 EU Member States, leading to uneven results for businesses across the Continent...’¹

Paragraph 1.74

On 16 February 2007, the DPA of the German federal state of Schleswig-Holstein awarded its privacy seal to the Windows online update procedure of Microsoft.²

Paragraph 1.82

On 20 June 2007, the Article 29 Working Party published a report on its first joint enforcement action.³ The action included a joint investigation of data controllers in the private health insurance sector carried out by the DPAs of Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovenia, the Slovak Republic, Spain, Sweden, and the United Kingdom.⁴ The investigation lasted thirteen months, and the Working Party found the results to be ‘positive’, noting that ‘one can assume that, in general, the processing of personal data by the private health insurance companies is in compliance with the principles and provisions laid down in

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

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

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

⁴ *Ibid*, 4.

Directive 95/46/EC on the protection of personal data'.⁵ At the same time, the Working Party announced its intention to carry out further such joint investigations, noting that they should 'become more like true audit actions, which require the power to directly verify the truthfulness of responses. It is furthermore necessary to institute random checks on the selected data controllers as an integral part of such investigations'.⁶ The Working Party also noted that the sectors to be examined in such audits would be selected based on an assessment of the data protection risks the sector poses, and the advantages of undertaking co-ordinated action at a European level.⁷

On 28 June 2007, the United States Department of the Treasury issued various representations describing controls and safeguards that the Treasury commits to use in accessing the SWIFT database.⁸ In a joint letter in reply, the European Commission and the Council of the European Union stated that 'Once SWIFT and the financial institutions making use of its services have completed the necessary arrangements to respect EC law, in particular through the provision of information that personal data will be transferred for commercial purposes to the United States and, as regards SWIFT, the respect of the 'Safe Harbour [sic]' principles, subject to lawful access by the US Treasury Department, SWIFT and the said financial institutions will be in compliance with their respective legal responsibilities under European data protection law.'⁹

Paragraph 1.88

On 15 June 2007, SWIFT announced that it would change the architecture of its data processing system so that intra-European data would be stored only in Europe (rather than in the US as was previously the case).¹⁰ While this cannot be considered an 'enforcement action', the change of architecture does demonstrate how EU data protection law can influence business decisions on a momentous scale.

Paragraph 1.97

On 7 March 2007, the European Commission adopted a communication on the work program for better implementation of the General Directive which the Commission had adopted in 2003.¹¹ In its Communication, the Commission concluded that implementation of the

⁵ Ibid, 7.

⁶ Ibid, 8.

⁷ Ibid.

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

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

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

¹¹ Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Commission document COM(2007) 87 final.

Directive had improved, although some Member States had still not properly implemented it.¹² The Commission also stated that the Directive should not be amended.¹³ Finally, the Commission noted several areas where it would work to improve implementation of the Directive, including the following: (1) continuing to work with Member States to ensure improved implementation; (2) producing interpretative communications on some provisions of the Directive; (3) encouraging all actors to reduce national divergences in implementation; (4) reviewing the impact of new technologies on data protection; and (5) dealing with the challenges posed by the demand for data processing based on public interest, particularly relating to law enforcement. On 25 July 2007, the European Data Protection Supervisor issued an opinion on the Commission's Communication which supported the Commission's conclusion that the Directive should not be amended at this time, but which seemed to see a more urgent need to improve its implementation by the Member States.¹⁴ In particular, the EDPS emphasized the importance of: (1) full implementation of the Directive; (2) considering the impact of technological developments on the Directive; (3) having a global perspective and further developing rules on international data transfers; (4) ensuring that personal data are protected despite law enforcement demands; (5) adopting more sectoral data protection legislation (for example, regarding RFID); (6) greater use of infringement procedures against the Member States; (7) encouraging the use of interpretative communications by the Commission to clarify important questions; (8) enhancing the use of non-binding instruments to increase compliance, such as privacy seals; and (9) better defining the role of institutional actors, in particular the Article 29 Working Party.

¹² Ibid, 5.

¹³ Ibid, 9.

¹⁴ 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive', available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf.

Chapter 2

Paragraph 2.25

In late 2006 and early 2007, the Article 29 Working Party adopted an opinion in the SWIFT affair,¹ as did a number of DPAs,² 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.³ 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 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

¹ 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.

² European Data Protection Supervisor (EDPS), ‘EDPS Opinion on the role of the European Central Bank in the SWIFT Case’, 1 February 2007; Datenschutzkommission [Austria], Bescheid Beschwerde, no. K121.245/009-DSK/2007, 21 March 2007; 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); Independent Centre for Privacy Protection at the Federal State of Schleswig-Holstein (ULD) (Germany), Opinion of 23 August 2006 (unofficial English translation); 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.

³ The National Bank of Belgium is the lead overseer, and cooperates with other G-10 central banks in oversight of SWIFT.

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,⁴ 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 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

⁴ Contrary to what has sometimes been erroneously stated, the US Patriot Act was not used as a legal basis for the subpoena.

for the form and contents of payment orders, introducing new services, etc.) without requiring the consent of banks.⁵

- SWIFT management decides autonomously on the level of information given to banks in relation to processing.⁶
- SWIFT provides added value for processing, such as the storage and validation of data and implementation of high-level security standards.⁷
- SWIFT management has the power to make critical decisions about processing (such as security standards and the location of databases).⁸
- 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.⁹
- 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.¹⁰
- SWIFT negotiates and terminates with full autonomy its services agreements, and also has full autonomy to change contracts and policies.¹¹
- 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.¹²

⁵ 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.

⁶ Article 29 Working Party, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’, 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; 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.

⁸ Ibid.

⁹ Datenschutzkommission [Austria], Bescheid Beschwerde, no. K121.245/009-DSK/2007, 21 March 2007, § 2b.

¹⁰ 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.

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

¹² 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.

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.¹³ 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.¹⁴
- 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.¹⁵
- 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.¹⁶
- SWIFT's role in complying with UST subpoenas does not change the analysis of its role as a data processor.¹⁷

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

¹³ 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.

¹⁴ 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.

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Ibid.

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 purpose and scope of the transfer of data to the UST'.¹⁸ 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,¹⁹ and yet the Canadian Federal Privacy Commission has

¹⁸ 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.

¹⁹ 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...'

since found that Canadian data privacy law (which has been recognized as ‘adequate’ by the EU²⁰) does not foreclose SWIFT from responding to a valid subpoena issued in the US.²¹

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.

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 2.83

In *Case of Copland v. The United Kingdom*,²² the European Court of Human Rights found that e-mails sent from work and personal internet usage of the employee of a public body were protected under Article 8 of the European Convention of Human Rights.

Paragraph 2.94

²⁰ 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.

²¹ 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’.

²² Application no. 62617/00 (3 April 2007) ECHR.

In one case, the Austrian data protection commissioner 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.²³

²³ 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. For example, any criticism that the alternative clauses results in a ‘lowering of the level of data protection’ (*Absenkung des Datenschutz-niveaus*) 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’,⁴ 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,⁵ 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.⁶

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 provisions of a directive.⁷ Moreover, all the authorities of a Member State must take,

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 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’.

⁵ 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.

⁶ ECJ, Case 249/85 *Albako* [1987] E.C.R. 2345, para. 17.

⁷ ECJ, Case 103/88 *Fratelli Costanzo* [1989] E.C.R. 1839, para. 33.

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.⁸ 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, or, failing this, to bring suit against the Commission under Article 230 of the EC Treaty, 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 4.61

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.

Paragraph 4.66

In June 2007, the European Commission announced that it had rejected a complaint raised by a Greek legislator that the transfer of personal data of the employees of the Greek subsidiary of the US company Abbott Laboratories violated EU data protection law. The Commission stated that Abbott's safe harbor membership meant that the transfer of the data to its headquarters in the US was not in breach of EU law.

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

⁸ 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.

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.⁹

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.¹⁰

Paragraph 4.124

Germany: On 1 June 2007, the DPA of the German federal state of Hessen approved the BCRs of Merck.¹¹ 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.¹²

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.¹³

⁹ 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.

¹⁰ Ibid.

¹¹ 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.

¹² 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.

¹³ 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 5.67

Consent of trade unions may be required for employee monitoring in Italy.¹ The Italian DPA has also issued guidelines for employee monitoring.²

Paragraph 5.68

The European Court of Human Rights has recognized that monitoring of employee communications may be legitimate under certain circumstances.³

Paragraph 5.84

The importance of adopting a formal policy for employee monitoring is demonstrated by the *Case of Copland v. The United Kingdom*.⁴ 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.⁵

Paragraph 5.93

On 7 March 2007, the French labor minister announced a consultation with trade unions and businesses about reforming the French Labor Code to allow for the implementation of whistleblower hotlines at the workplace. The announcement follows a report prepared by the University of Montpellier and AREVA Groupe, calling the Government to amend the Labor Code to introduce specific provisions to regulate the use of whistleblower systems by

¹ See Linkomies, 'Employee monitoring in Italy often requires trade union consent', (August 2006) *Privacy Laws & Business International Newsletter* 21.

² '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.

³ 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'.

⁴ *Ibid.*

⁵ 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.'

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.⁶

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 in Germany.⁷

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.⁸
- On 1 January 2007, new whistleblower provisions adopted by the Norwegian DPA entered into force.⁹
- In the summer of 2007, the Spanish DPA adopted a paper regarding the implementation of whistleblower systems in companies.¹⁰

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

⁶ 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.

⁷ 'Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz', available (in German) at <http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationssysteme/wirtschaft/whistleblowing.html>.

⁸ 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>.

⁹ A summary is available in English at http://www.datatilsynet.no/templates/Page_1857.aspx.

¹⁰ Informes jurídicos No. 2007-0128, available (in Spanish) at https://www.agpd.es/upload/Canal_Documentacion/Informes%20Juridicos/Otras%20cuestiones%20de%20interés/OC%20%282007-0128%29%20%28Creación%20de%20sistemas%20de%20denuncias%20internas%20en%20las%20empresas%20C%20mecanismos%20de%20whistleblowing%29.pdf.

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.¹¹

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.¹²

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

¹¹ Oberlandesgericht Düsseldorf, Decision of 13 April 2006, no VI-U(Kart) 23/05.

¹² 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.

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.¹³

- In January 2007, the Greek Authority for the Information and Communication Security and Privacy fined Vodafone €76 million over a security breach and wiretapping scandal involving the illegal monitoring of the mobile calls of top government officials such as the Prime Minister and the Foreign Minister. Vodafone was ruled at fault for not preventing unknown hackers from subverting a legitimate surveillance system, supplied by Ericsson, to spy on Greek officials around the time of the 2004 Athens Olympics. Calls from and to targeted phones were relayed to sixteen mobile phones using pre-paid cards, located in central Athens, thanks to unauthorized manipulation of the Ericsson-supplied surveillance software used by Vodafone Greece. The Authority said that Vodafone had failed to take adequate measures to protect its network and had not informed subscribers that their phones were being tapped. It further criticized Vodafone for obstructing its investigation by failing to admit the existence of the surveillance system itself.
- In February 2007, the UK financial services regulator, the Financial Services Authority (FSA), fined the UK's largest building society, Nationwide, £ 980,000 following the theft of an employee's laptop.¹⁴ 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

¹³ The CNIL's decision can be found (in French) at <http://www.cnil.fr/index.php?id=2165>.

¹⁴ 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.

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.¹⁵ 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.

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

Paragraph 5.148

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

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

Paragraph 5.151

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

¹⁵ Further information is available at http://www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf.

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.

A good 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 14

Documents Adopted by Article 29 Working Party (from September 2006 through June 2007)

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

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