

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 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

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.

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 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

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

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 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

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.

- 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
- 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

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.

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.

- 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
- 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

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Ibid.

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'.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

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

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 2.37

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

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’.

²³ See also Appendix 13.

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 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.

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.

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).

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

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

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.

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