01935/06/EN
WP128

Opinion 10/2006
on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Adopted on 22 November 2006

Executive Summary

This opinion of the Article 29 Working Party contains the findings on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

In this context, the Article 29 Working Party emphasizes that even in the fight against terrorism and crime fundamental rights must remain guaranteed. It insists therefore on the respect of global data protection principles.

SWIFT is a worldwide financial messaging service which facilitates international money transfers. SWIFT stores all messages for a period of 124 days at two operation centres, one within the EU and one in the USA – a form of data processing referred to in this document as "mirroring". The messages contain personal data such as the names of the payer and payee. After the terrorist attacks of September 2001, the United States Department of the Treasury ("UST") issued subpoenas requiring SWIFT to provide access to message information held in the USA. SWIFT complied with the subpoenas, although certain limitations to UST access were negotiated. The matter became public as a result of press coverage in late June and early July 2006.

As a Belgian based cooperative, SWIFT is subject to Belgian data protection law implementing the EU Data Protection Directive 95/46/EC ("the Directive"). Financial institutions in the EU using SWIFT's service are subject to national data protection laws implementing the Directive in the Member State in which they are established.

The Working Party concludes that:

- Both SWIFT and instructing financial institutions share joint responsibility, although in different degrees, for the processing of personal data as "data controllers" within the meaning of Article 2(d) of the Directive.
- Continued processing of personal data, knowing the large scale of the UST subpoenas, is a further purpose which is not compatible with the original commercial purpose for which the personal data have been collected, within the meaning of Article 6(1)(b) of the Directive.
- Neither SWIFT nor the financial institutions in the EU have provided information to data subjects about processing of their personal data, in particular as to the transfer to the USA, as required under Articles 10 and 11 of the Directive.
- The control measures put in place by SWIFT, in particular regarding UST access to the data, in no way replace the independent scrutiny that could have been provided by supervisory authorities established under Article 28 of the Directive.
- As far as the transfer to the US operating centre is concerned, SWIFT cannot rely on Article 25 of the Directive to legitimate the processing.
- None of the derogations in Article 26 (1) of the Directive apply to the processing of data in the USA.
- SWIFT did not make use of the mechanisms under Article 26(2) of the Directive to obtain authorisation from the Belgian data protection supervisory authority for the processing operations.
- The Article 29 Working Party calls upon SWIFT and the financial institutions to take measures in order to remedy the currently illegal state of affairs without delay.
- Furthermore the Article 29 Working Party calls for clarification of the oversight on SWIFT.

The Article 29 Working Party will follow-up and monitor all of the above.

TABLE OF CONTENTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

has adopted the present Opinion:

1. BACKGROUND

The independent data protection supervisory authorities within the European Union[2] are assessing a major question relating to the transfer of financial data on a large scale from a company based in the European Union (SWIFT) to the US authorities. The details and conditions of such transfers, in particular the processing of personal data relating to individuals in Europe, have raised the concerns of DPAs who have joined forces in the investigation of the data flow and the analysis of its compliance with European privacy principles, in particular with the Data Protection Directive ("the Directive").

1.1. Sequence of events

At the end of June and beginning of July 2006, press coverage in the European and US media questioned the role and responsibilities of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in relation to the transfer of personal data to the Office of Foreign Assets Control (OFAC) of the United States Department of the Treasury ("UST"). SWIFT is a Belgian based cooperative active in the processing of financial messages. It was revealed that personal data, collected and processed via the SWIFT network for international money transfers using the bank identification code ("BIC") or "SWIFT" code, had been provided to the UST since the end of 2001 on the basis of subpoenas under American law for terrorism investigation purposes.

---

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[2] In addition to the EU authorities, other data protection supervisory authorities have started investigations on this issue: Australia, Canada, New Zealand, Switzerland, Iceland.

SWIFT released a first statement[3] on 23 June 2006 pursuant to this press coverage. According to its press statement, SWIFT is "the industry-owned cooperative supplying secure, standardized messaging services and interface software to over 7,800 financial institutions worldwide."

The European Commission decided to follow this case closely and asked the Belgian authorities in July 2006 for information about the conditions under which SWIFT processes personal data and whether it complies with Belgian data protection legislation implementing Directive. The Commission is also verifying with Member States whether banks making use of SWIFT for execution of payments orders comply with their national laws on data protection with respect to their processing of personal data relating to such payments.

By resolution of 6 July 2006[4], the European Parliament asked the Member States to ensure and verify that there is no legal lacuna at national level and that Community data protection legislation also covers central banks. In this resolution, the European Parliament also expressed serious concerns as to the purposes of the transfer of data to the UST. It also strongly disapproved of "any secret operations on EU territory" that affects the privacy of EU citizens. It furthermore declared that it is deeply concerned that such operations should be taking place without the citizens of Europe and their parliamentary representation having been informed. It finally urged the USA and its intelligence and security services to act in a spirit of good cooperation and notify their allies of any security operations they intend to carry out on EU territory. The possibility of transfers linked to "illegal activities" was raised but also of transfers of "information on the economic activities of the individuals and countries concerned", which "could give rise to large-scale forms of economic and industrial espionage". The resolution requested the Member States to transmit the results of their verification to the European Commission, the Council and the European Parliament.

On 27 July 2006, the Chairman of the Article 29 Working Party announced that the European data protection authorities had decided to coordinate their activities. In a subsequent meeting on 26 and 27 September 2006, the Article 29 Working Party held a first plenary discussion.[5]

On 4 October 2006, at a public hearing held by the European Parliament's Civil Liberties and Economic and Monetary Affairs committees, the issue was discussed with, amongst other participants, the Chief Financial Officer of SWIFT and the European Central Bank[6].

---

[3] "SWIFT statement on compliance policy", published on http://www.swift.com/index.cfm?item_id=59897

[4] European Parliament resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA-PROV(2006)0317)

[5] Article 29 Working Party press releases: Press Release of the Article 29 Working Party on Swift Case of 28/7/2006: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_28_07_06_en.pdf; Press Release on the SWIFT Case of 27/9/2006; http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf .

[6] The full public hearing exchanges can be found at http://www.europarl.europa.eu/news/expert/infopress_page/017-11292-275-10-40-902-20061002IPR11291-02-10-2006-2006-false/default_en.htm

The European Data Protection Supervisor issued some preliminary comments on his investigation into the role of the European Central Bank (ECB) pursuant to Regulation (EC) 45/2001.[7]

At national level, data protection supervisory authorities contacted their relevant banking organizations.

The Data Protection Authority (DPA) of Belgium carried out an inquiry into the legality of the data processing by SWIFT. In the course of this inquiry, the Belgian DPA made direct contact with SWIFT to determine both the scope and scale of the monitoring and the data transfers. The Belgian DPA established in its decision of 27 September 2006 that the transfer by SWIFT of personal data to SWIFT's US branch is in breach of the Belgian law of 8 December 1992 concerning the protection of privacy with regard to data processing of a personal nature[8]. In particular the Belgian DPA found that SWIFT infringed essential provisions relating to the obligations of information, limitation of the purpose of the data processing activities and transfer of the personal data to third countries. The Belgian DPA established that SWIFT made a *"hidden, systematic, massive and long-term violation of the fundamental European principles as regards data protection"*.

On the basis of the information gathered during these investigations the Working Party wishes to analyze the compliance by SWIFT with the data protection principles that are contained in the Directive and implemented in all Member States by national data protection laws with a broad scope of application.

SWIFT sent a copy of its replies to the Belgian, Spanish and French DPA to the Chairman of the Article 29 Working Party[9].

1.2. Facts

1.2.1. SWIFT data processing activities in figures

SWIFT processes an average of 12 million messages on a daily basis[10]. The total volume of messages processed amounted, e.g. in the year 2005, to 2.5 billion messages, of which 1.6 billion were for Europe and 467 million were for the Americas. The information processed by SWIFT concerns messages on the financial transactions of hundreds of thousands of EU citizens. European financial institutions (not limited to banks) use the SWIFTNet FIN Service for the worldwide transfer of messages in relation to financial transfers between financial institutions. This transfer occurs regardless of whether the messages are processed within the European Union (EU) and the European Economic Area (EEA) or in a third country.

---

7 http://www.edps.europa.eu/Press/EDPS-2006-10-EN%20swift.pdf

8 http://www.privacycommission.be/communiqu%E9s/AV37-2006.pdf

9 SWIFT letter to Chairman of the Article 29 Working Party of 31 July 2006.

10 SWIFT Annual report 2005; available at http://www.swift.com/index.cfm?item_id=59684 .

1.2.2. Categories of data processed

The messages that are transmitted via the SWIFTNet FIN service contain personal data such as the names of the beneficiary and the ordering customer. Payment related messages may however include more information such as a reference number to allow payer and payee to reconcile the payment with their respective accounting documents. In addition, certain message types allow for unstructured text information to be included.

Apart from sales offices in various countries, SWIFT has two operation centres located in SWIFT branches, one in a Member State of the EU and one in the United States. In these operation centres, as part of the SWIFTNet FIN service, all messages processed by SWIFT are stored and mirrored for 124 days, as a "back-up recovery tool" for customers in case of disputes between financial institutions or data loss. After this period the data is erased.

1.2.3. Subpoenas by the UST

Since the terrorist attacks of September 2001, the UST has addressed multiple administrative subpoenas to the SWIFT operation centre in the US. After enquiry, SWIFT stated that to date it had received and complied with 64 UST subpoenas.

Under US law, an administrative subpoena is an order from a government official to a third party, instructing the recipient to produce certain information.[11] The scope of the UST subpoenas in this case is materially, territorially and in time very wide and is defined in the subpoenas and in the correspondence on the negotiations between the UST and SWIFT. These subpoenas are issued for any transactions which relate or may relate to terrorism, relate to *x* number of countries and jurisdictions, on *y* date, or "*from ... to ...*" dates ranging from one to several weeks, within and outside the US. It concerns messages of inter-bank transactions within the US, to or from the US, as well as messages from outside the US, such as messages within the EU.[12]

SWIFT privately negotiated an arrangement with the US Treasury on how to comply with the subpoenas. Through this process, SWIFT claims to have received *"significant protections and assurances as to the purpose, confidentiality, oversight and control of the limited sets of data produced under the subpoenas"*[13].

According to the findings of the Belgian DPA, the practical communication of personal data to the UST is performed by the SWIFT operating centre in the US in several steps. There is no direct extraction of individualised data mirrored in the SWIFT database, but instead, SWIFT negotiated a "black box" construction with the UST that permitted a

---

[11] Hearing before the United States Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security:"Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists" Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice, June 22, 2004; http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf

[12] Cf. Opinion Belgian DPA, B.2 (unofficial EN translation), footnote 8.

[13] "SWIFT statement on compliance policy", published on http://www.swift.com/index.cfm?item_id=59897.

transfer of data from the mirrored SWIFT database to the “black box”. Once the data are in the "black box", which is owned by the US, the UST performs focused searches.

Further details on the communication of personal data to the UST were disclosed to the DPA in Belgium and can be found in its opinion[14].

2. APPLICABLE DATA PROTECTION FRAMEWORK

2.1. Applicability of Directive 95/46/EC

Since personal data are contained in the messages that are transmitted via the SWIFTNet FIN service, the Working Party finds that the Directive is applicable to the processing of personal data via the SWIFTNet FIN service.

The Working Party stresses that the fact that the processing of personal data is incidental to the provision of a service is not relevant to the determination of an organisation's capacity as a data controller. The definitions of “processing of personal data” and “personal data” are clearly defined in Article 2 of Directive. Where the activities carried out by an entity fall under these definitions, the Directive applies and therefore the data processing activities shall be carried out in full conformity with the Directive.

2.2. Law applicable to SWIFT

Article 4(1)(a) of the Directive states that each Member State shall apply the national provisions it adopts pursuant to the Directive to the processing of personal data where “(…) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State”.

The head office of SWIFT is located in La Hulpe, Belgium. SWIFT also has two operating centres (one in Europe and one in the US, which act as a complete mirror). In addition, SWIFT has several sales offices in the UK, France, Germany, Italy, Spain, etc. The critical decisions on the processing of personal data and transfer of data to the UST were decided by the head office in Belgium.

As a consequence, the processing of personal data by SWIFT is subject to Belgian law, implementing the Directive, regardless of where the data processing takes place.

2.3. Law applicable to the financial institutions

With regard to the processing operations for which the financial institutions which make use of SWIFT’s service for their international payment orders can be considered as controllers, the applicable national law is determined by Article 4(1)(a) of the Directive and, with regard to Community institutions and bodies, Article 3 of Regulation (EC)

[14] See footnote 8.

45/2001[15]. This means that, in the case of financial institutions, different – though harmonized – laws are applicable.

The Working Party stresses that, since personal data are being processed in financial transactions regarding hundreds of thousands of citizens via institutions established in the EU (the cooperative SWIFT as well as financial institutions making use of the SWIFTNet FIN service), the national laws on data protection – adopted in implementation of the Directive – of the different Member States concerned are applicable.

3. ROLE OF SWIFT AND OF THE FINANCIAL INSTITUTIONS

According to the Directive, the controller has to ensure that the obligations with respect to the processing of personal data are complied with.

The question is whether SWIFT and/or the financial institutions are to be considered as data controllers or as processors.

According to the definitions of the Directive, 'controller' means "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" (Article 2 (d));a 'processor' means "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (Article 2 (e)).

3.1. Role of SWIFT

SWIFT has always presented itself as being "*solely a messaging intermediary for transmitting secure and confidential financial messages between financial institutions. SWIFT is not a bank, nor does it hold accounts of any customers*." This presentation also formed the basis for the assessments carried out by some DPAs in Member States when authorizing data processing activities by their banks.

The international service structure of SWIFT and the contractual arrangements that have been made between SWIFT and financial institutions are rather complex. The Working Party points out, however, that this type of structure including the role of a service provider working together with other actors is not unique. The SWIFT structure appears to be an example of a formal cooperative network. SWIFT was organized in 1973 by a group of European banks which wanted to develop a new method to send payment instructions to correspondent banks in a standardized manner. To this effect, a cooperative company with limited liability was established under Belgian law.

The Working Party refers to similar cases of cooperative networks such as the case of the Terminated Merchant Databases that are operated by VISA and Mastercard in cooperation with financial institutions in order to analyze the risks associated with

---

[15] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ L 8, 12.1.2001, p. 1.

signing up a particular merchant with the VISA or Mastercard system[16]. The Working Party also makes reference to the cases of clearing and settlement of transactions systems and to passenger reservation systems where travel agencies and airline companies on the one hand and the managers of those systems (such as Galileo) on the other hand have differing responsibilities.

Independently of the contractual relationship between SWIFT and the financial institutions under civil or commercial law, which may include the term "subcontractor", from the point of view of data protection, SWIFT is not a simple "subcontractor" or processor within the meaning of Article 2 of the Directive for the normal processing of personal data for its usual commercial purpose. The facts illustrate that SWIFT has evolved in the last few decades and does more than just act on behalf of its clients. Even if it was assumed for a moment that SWIFT acted as "processor", SWIFT has taken on specific responsibilities which go beyond the set of instructions and duties incumbent on a processor and cannot be considered compatible with its claim to be just a "processor".[17] The management of SWIFT operates in the context of a formal cooperative network which determines both the purposes and the means of data processing within the SWIFTNet Service and what personal data is processed via that service. The management of SWIFT decides autonomously on the level of information that is provided to the financial institutions in relation to the processing. SWIFT management is able to determine the purposes and means of the processing by developing, marketing and changing the existing or new SWIFT services and processing of data, e.g. by determining standards applicable to it clients as to the form and content of payment orders, without requiring the consent of the financial institutions. SWIFT also provides added value for the processing of personal data, such as the storage and validation of personal data and the protection of personal data with a high security standard. SWIFT management has the power to take critical decisions with respect to the processing, such as the security standard and the location of its operating centres. Finally, SWIFT management negotiates and terminates with full autonomy its services agreements and drafts and changes its various contractual documents and policies[18]. The above are the practical and legal means of the processing.

For the transfer of personal data to the UST, SWIFT decided to comply with the US subpoenas. It also took the initiative to negotiate in a non-transparent manner, through correspondence and a comfort letter with the UST, the conditions for passing the personal data to the UST. It deliberately decided not to inform the financial institutions concerned of this negotiation. Indeed, the control mechanisms obtained and operated by SWIFT affected the purpose and scope of the transfer of data to the UST. These actions exceed by far the normal capacities of a data processor in view of its supposed absence of autonomy with respect to the instructions of the data controller.

---

16 See e.g. Article 29 Working party "Guidelines for Terminated Merchant Databases"; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf.

17 Data processors must in any case comply with the Directive, see e.g. Art. 17 (3) on security measures.

18 Cf. clause 4.5.3 of the general terms and conditions states: "the customer shall have been deemed to have consented to any such processing…".

While SWIFT presents itself as a data processor, and some elements might suggest that SWIFT has acted in the past as a processor in certain cases on behalf of the financial institutions, the Working Party, having considered the effective margin of manoeuvre it possesses in the situations described above, is of the opinion that SWIFT is a controller as defined by Article 2 (d) of the Directive, for both the normal processing of personal data under its SWIFTNet service as well as for the further processing by onward transfer of personal data to the UST.

3.2. Role of the financial institutions

The role of the financial institutions in the use of the SWIFTNet FIN service needs to be assessed. Some financial institutions were not fully informed by SWIFT of the volume and exact characteristics of the processing and mirroring of the personal data, including the further transfer of the mirrored personal data to the UST, However, after the disclosure of these facts on and after 23 June 2006, all financial institutions are aware of the situation when sending personal data via the SWIFTNet FIN service for international money transfers.

Financial institutions using SWIFT are supposed and expected to retain some influence on the policy of the cooperative. Some financial institutions are present on SWIFT's Board of Directors and the current management structure of SWIFT was originally designed to enable banks and financial institutions to retain some power over SWIFT decision-making processes. These institutions should therefore be considered as taking part in the determination of the purpose and means of the processing, with the cooperative of which they are members. They have also direct contact with the concerned natural persons, and they play an essential role in the execution of the international payment orders of their clients.

It is also important to keep in mind that the financial institutions are autonomous and that they can pursue their own objectives at an inter-bank level. The Working Party notes that, within the inter-bank traffic, the financial institutions often make crucial decisions on the transmission of personal data to SWIFT, often without the knowledge of their clients. This is shown by the following elements:

- On the inter-bank level, the financial institutions often decide autonomously about the means used when settling payment instructions. They can use or develop alternative or rival services for the transmission of these financial messages within the inter-bank system (e.g. e-mail, fax, telephone). Choices at this level will determine the global privacy characteristics regarding payment instructions settled by the financial institutions. When choosing an inter-bank service, the financial institutions are, in view of the diversity of the services at inter-bank level, free to be guided by elements other than information security - which is of course always a requirement - such as, the privacy policy of the professional service provider. The financial institutions have the option to use a strict privacy policy from a particular provider or use a solution such as virtual private network as a guarantee in order to safeguard the trust of their clients and their services to the maximum.
- Financial institutions adhere to and accept the contractual framework of the

SWIFTNet FIN service[19]. The contractual documentation (Data Retrieval Policy[20]), and the SWIFT compliance policy make SWIFT customers aware of the general principle to transfer personal data subjected to subpoenas either served on them or on SWIFT. According to the Opinion of the Belgian DPA, SWIFT argued that the number of subpoenas addressed to financial institutions could run into thousands or even tens of thousands per year. It is therefore doubtful that financial institutions which are active on the international payments market would be unaware of the general principle of subpoenas.

- The financial institutions must assess the possible implications and privacy risks, including privacy risks for their clients relating to the SWIFTNet FIN service, which they, as a professional service provider, sign up to. It is therefore important to check whether the privacy policy of the instructing institution contains clauses relating to these risks.
- Considering the fact that the financial institutions are acting on behalf of their clients giving payment instructions, they are not allowed to pass on the necessary data to other purposes than strictly payment transfer. If it is known to a financial institution, that SWIFT uses data entrusted to them also in ways which are not strictly payment transfers and nevertheless continues to make use of the SWIFT services, the question of the legal basis for such transfer and use must be put: unless there is a special agreement between financial institution and their clients it does not seem justified to entrust banking data to SWIFT for other purposes than the mere service acknowledged.

As a consequence, financial institutions are not only controllers in the meaning of Article 2 (d) of the Directive as to their own data processing activities but they also bear some responsibility as regards the data processing activities of SWIFT. The fact that the management structure of the SWIFT cooperative appears to have evolved over time to the point that SWIFT's management would have grown more independent than originally intended does not prevent its founders, i.e. the financial institutions, from retaining their qualification as data controllers in the sense of the Directive.

On the basis of the above elements, the Working Party is of the opinion that sufficient elements support the opinion that a joint responsibility exists with the financial institutions and the cooperative SWIFT where they are represented, for the processing of personal data via the SWIFTNet FIN service. However joint responsibility does not necessarily mean equal responsibility. Whilst SWIFT bears primary responsibility for the processing of personal data in the SWIFTNet FIN service, financial institutions also bear some responsibility for the processing of their clients' personal data in the service.

---

[19] Part of the contractual documentation is the "SWIFT User Handbook" which contains the standardised message types to be used.

[20] Where it is stipulated: "*For the avoidance of any doubt, nothing in this policy or, more generally, SWIFT's obligations of confidence to customers, shall be construed as preventing SWIFT from retrieving, using, or disclosing traffic or message data as reasonably necessary to comply with a bona fide subpoena or other lawful process by a court or other competent authority*." Cf. Opinion Belgian DPA, D.2, footnote 8.

3.3. Role of central banks

The involvement of central banks must be examined, taking account of the different roles they play as regards SWIFT and as regards the oversight within the area of financial payments. Firstly, SWIFT is subject to cooperative oversight by the Central Banks of the Group of Ten countries (G-10 Group)[21]. The oversight focuses primarily on ensuring that SWIFT has effective controls and processes to manage risks for the financial stability and the soundness of financial infrastructures. Furthermore, "overseers review SWIFT's identification and mitigation of operational risks, and may also review legal risks, transparency of arrangements and customer access policies. SWIFT's strategic direction may also be discussed with the Board and senior management"[22]. The major instrument for the oversight of SWIFT is the influence and pressure that may be applied by the overseeing authority ("moral suasion"). Overseers can formulate recommendations to SWIFT; however, it is also clear that the oversight of SWIFT does not grant SWIFT any certification, approval or authorisation by the Central Banks.

Provisions on the confidential treatment of non-public information are included in Memorandums of Understanding between SWIFT and the Central Banks.

The G-10 Group was informed in the course of 2002 about the data transfers to US authorities. However, the Group considered that this issue fell outside the scope of its oversight role. Furthermore, many central banks interpreted Memorandums of Understanding on confidentiality as preventing them from referring this issue to competent authorities at national and European level. Therefore, the G-10 Group neither addressed the consequences on data protection of the transfers to US authorities, nor did they inform the relevant authorities nor did they urge SWIFT to do so.

Furthermore, the President of the European Central Bank (ECB) stated at the public hearing at the European Parliament that the G-10 Central Banks "*did not give SWIFT any blessing in relation to its compliance with these subpoenas. In fact, we could not have given any such authorisation even if we had wanted to, as this fell outside our competence. Therefore, SWIFT remained solely responsible for its decisions*".[23]

Secondly, it shall be highlighted that the limited role that the Central Banks currently play in SWIFT oversight does not exclude that also a Central Bank might be considered – as any other financial institution using SWIFTNet service – as a (joint) controller whenever it acts as a SWIFT customer (see above, paragraph 3.2), in the event that they process personal data for the purpose of inter-bank transactions. In this perspective, the fact that some Central Banks were informed of the data transfers to US authorities might

---

[21] The G-10 Group is composed by the National Bank of Belgium, Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d' Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.

[22] Financial Stability Review 2005, published by the National Bank of Belgium and available on its web site www.nbb.be.

[23] Jean-Claude Trichet: Statement by the President of the ECB at the public hearing at the European Parliament on the interception of bank transfer data from the SWIFT system by the US secret services.

be considered as relevant in order to determine their responsibility as users of the SWIFT system.

4. ASSESSMENT OF THE COMPATIBILITY WITH DATA PROTECTION RULES

4.1. Application of the principles of data quality and proportionality (Article 6 of the Directive)

In accordance with Article 6 of Directive, personal data must be processed fairly and lawfully;[24] they must be collected for specified, explicit and legitimate purposes[25] and not be processed for purposes incompatible with the original one for which they were collected. Moreover, the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[26] Combined, these latter rules are referred to as the "proportionality principle". Finally, appropriate measures have to be taken to ensure that data which are inaccurate or incomplete are erased or rectified.[27]

4.1.1. Commercial purpose

The personal data was collected by the financial institutions only for the purpose of processing the client's payment orders and subsequently by SWIFT for the purpose of executing the SWIFTNet FIN service (commercial purpose). This commercial purpose for the processing of personal data can therefore be considered as the only specified, explicit and legitimate purpose.

As to the transfer of personal data to third countries, see below under section 4.6

4.1.2. Further processing for incompatible purposes

aa) Personal data may not be processed for purposes which are incompatible with the original purpose. By deciding to mirror all data processing activities in an operating centre in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law.

In this case, SWIFT received subpoenas issued by the UST for alleged terrorism investigations. This further purpose is completely different from the original purpose and its treatment of the personal data involved, and may have direct consequences for the individuals whose personal data are being processed. This further purpose is not compatible with the original, commercial-only purpose for which personal data have been collected.

---

[24] Article 6(1)(a) of the Directive.

[25] Article 6(1)(b) of the Directive.

[26] Article 6(1)(c) of the Directive.

[27] Article 6(1)(d) of the Directive.

SWIFT was aware of this further purpose. The SWIFT management endorsed it and cooperated. SWIFT has not pointed this purpose out, neither to the users of its services nor to any data protection supervisory authority.

bb) It has also been established that massive data transfers took place from SWIFT to the UST, without an effective possibility to check the individualized character of the data requested. According to SWIFT, all financial messages could potentially be scrutinized via the "black box" system by the UST. This system allows the UST to retrieve from the "black box" all messages – and the personal data contained therein – it deems necessary.

The Working Party points out that even for the purposes of alleged terrorism investigations only specific and individualized data should be transferred by SWIFT on a case by case basis, in full compliance with data protection principles. As this is not the case, the current practice is not proportionate and thereby violates Article 6 (1) (c) of the Directive.

cc) Article 13 provides that "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1) [as the purpose limitation principle], 10, 11(1) [duty to inform the data subject], 12 [right of access] and 21 [publicizing of processing operations] when such a restriction constitutes a necessary measure to safeguard [a list of important public interests which follows] (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences [...]; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);".

The European Court of Justice (ECJ) has cast some light on the understanding of these provisions. On joined cases C-465/00, C-138/01 and C-139/01 ("Rechnungshof") of 20 May 2003, the Court made clear that the communication of data originally collected for "economic" purposes to third parties, including public authorities "constitutes an interference within the meaning of Article 8 ECHR". Further, derogations from the principle of purpose limitation laid down in the Data Protection Directive need to respect Article 13 of that directive, and for that they need to be "justified from the point of view of Article 8 of the Convention" (Rechnungshof, C-465/00, §68 ff).

According to the Convention, in order for an interference with the right to private life to be justified, it needs to be done "in accordance with the law" and be "necessary in a democratic society" for a public interest purpose. The Strasbourg jurisprudence has repeatedly reminded that the Law providing for the interference "must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

However, these provisions cannot be invoked as SWIFT did not comply on these issues with the Belgian law.[28]

28

dd) The Working Party moreover points to the existence of legal structures on governmental level. The Working Party emphasizes that systems should be used in compliance with the bank secrecy principle. It refers in this respect to the 40+9 recommendations of the Financial Action Task Force (FATF/GAFI), an inter-governmental body created in 1989 whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The Working Party also refers to the system of exchange of financial information put in place between the respective national financial intelligence cells of 96 countries (Egmont Secure Web, ESW), coordinated by FinCEN in the United States. In this framework, financial information can be given to the requesting party in compliance with the national rules of the country exporting the information.

The Working Party also refers to existing cooperation mechanisms set up or developed under the third pillar (judicial and police cooperation), and in particular the international agreements signed on 25 June 2003 between the US and the EU[29] on mutual legal assistance and, although more remotely to this subject, the international agreement on extradition. Although these treaties are not yet ratified, according to Article 18 of the Vienna Convention on the Law of Treaties[30], a State is obliged to refrain from acts which would defeat the object and purpose of a treaty when it has signed the treaty or has exchanged instruments constituting the treaty subject to ratification, as long as it has not notified an intention not be become a party to the treaty.

As a result by having decided to mirror all data processing activities in an operating centre in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law and where a processing of personal data has been organized in a way that appears to circumvent the structures and international agreements already in place.

Overall, the Working Party is of the opinion that the principles of purpose limitation and compatibility, proportionality and necessity of the personal data processed are not respected.

4.2. Legitimacy (Article 7 of the Directive)

For any personal data processing to be lawful, it needs to be legitimate and satisfy one of the grounds set out in Article 7 of the Directive.

---

[29] Agreement on extradition between the EU and the US" and the "Agreement on mutual legal assistance between the EU and the US".
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf and
http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20european%20union%22

[30] Treaty of Vienna on the law of treaties of 23 May 1969. The United States have signed this treaty.

4.2.1. Necessary for the performance of a contract (Article 7 (b) of the Directive)

SWIFT processes the personal data contained in the messages in the SWIFTNet Fin service in order to execute payment orders entrusted to SWIFT by the financial institutions only.

However, even if in this context such processing for this commercial purpose could be considered necessary for the execution of the agreement between SWIFT and the financial institutions concerned, the way it was done by mirroring the personal data in the US operations centre is not acceptable for other reasons which are discussed later at 4.6 .

4.2.2. Necessary for compliance with a legal obligation to which the controller is subject (Article 7(c) of the Directive)

The processing and mirroring could have been necessary for compliance with a legal obligation to which the controller is subject.

SWIFT, with its headquarters in Belgium, did not formally invoke a legal basis within Belgian or European law for this particular processing. The Working Party further notes that is no legal obligation imposed by Belgian or European law for this particular data processing activity. In addition, the Working Party already stated in its "SOX opinion"[31] that *"an obligation imposed by a foreign legal statute or regulation (...) may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive"*. The Working Party considers that this reasoning also fully applies in this case.

Article 7 (c) of the Directive can therefore not be used to justify the processing and mirroring of the personal data in this case.

4.2.3. Necessary for the purposes of a legitimate interest pursued by the controller (Article 7(f) of the Directive)

According to Article 7(f) of the Directive, the processing and mirroring could be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

The question is whether Article 7 (f) of the Directive could be used to justify the processing and mirroring, with the consequence that the processing operations in its US operations centre are subject to US subpoenas.

---

[31] Opinion 1/2006 on the application of the EU data protection rules to internal wistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against, banking and financial crime.

It cannot be denied that SWIFT has a legitimate interest in complying with the subpoenas under US law. If SWIFT did not comply with these subpoenas, it runs the risk of incurring sanctions under US law. On the other hand, it is also crucial that a "proper balance" is found and respected between the risk of SWIFT being sanctioned by the US for eventual non-compliance with the subpoenas and the protection of the rights of individuals.

Article 7 (f) of the Directive requires a balance to be struck between the legitimate interest pursued by the processing of personal data and the fundamental rights of data subjects. This balance of interest test should take into account issues of proportionality, subsidiarity, the seriousness of the alleged offences that can be notified and the consequences for the data subjects. In the context of the balance of interest test, adequate safeguards will also have to be put in place. In particular, Article 14 of the Directive provides that, when data processing is based on Article 7(f), individuals have the right to object at any time on compelling legitimate grounds to the processing of the data relating to them.

SWIFT conducted the processing and mirroring of its data in a "hidden, systematic, massive and long-term"[32] manner, without having specified the further incompatible purpose at the time of processing the data, and without SWIFT pointing this purpose out to the users of its services. This further processing and mirroring for an incompatible purpose could have far-reaching effects on any individual.

The Working Party therefore considers that the interests for fundamental rights and freedoms of the numerous data subjects override SWIFT's interest not to be sanctioned by the US for eventual non-compliance with the subpoenas.

4.3. Provision of clear and complete information about the scheme (Articles 10 and 11 of the Directive)

According to Articles 10 and 11 of the Directive, the controller is obliged to inform data subjects about the existence, purpose and functioning of its data processing, the recipients of the personal data and the right of access, rectification and erasure by the data subject. All clients of financial institutions, regardless of their nationality or country of residence, have a right to know what happens to their "confidential" data.

The Working Party observes that this information concerning the processing and mirroring in the US operations centre was not provided, neither by SWIFT, nor by the financial institutions concerned.

According to Article 13 of the Directive, EU Member States may adopt legislative measures to restrict the scope of some of the obligations and rights provided for in the Directive. Such a restriction must constitute a necessary measure to safeguard, e.g. the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions, on a case-by-case basis and only if that interference is

---

[32] Opinion Belgian DPA, cf footnote 8.

justified from the point of view of Article 8 of the European Convention of Human Rights. However such a general, long and large-scale operation without any information provided at all would not be in line with Article 13.

4.4. Compliance with notification requirements (Article 18 to 20 of the Directive)

Data controllers have to comply with the requirements of Articles 18 to 20 of the Data Protection Directive as regards notification of their data processing activities to, or prior checking by, the national data protection authorities.

In Member States providing for such a procedure, the processing operations might be subject to prior checking by the national data protection authority in as much as those operations are likely to present a specific risk to the rights and freedoms of the data subjects. The evaluation of whether such processing operations fall under prior checking requirements depends on the national legislation and the practice of the national data protection authority.

The Working Party notes that SWIFT did notify some types of processing to the Belgian DPA[33] but did not notify the processing and mirroring in the US operations centre for the execution of international payment orders and neither the further purpose.

4.5. Oversight mechanisms

The establishment in EU Member States of data protection supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data. This principle of complete independence of the supervisory authority is laid down in Article 28 of the Directive.

Due to the lack of information by SWIFT, the financial institutions and the overseers to the national data supervisory authority, the existing data protection control mechanisms of the Directive could not be effectively applied. The Working Party regrets that no prior consultation, formal or informal, was effected by SWIFT or the financial institutions with the data protection authorities in relation to the processing and mirroring of personal data in the US operations centre.

Verifications by the national authorities show that for the transfer of SWIFT data to the UST for the further purpose the control measures that were put in place by SWIFT mainly consisted of private audit controls by a consultant company, and the review by SWIFT employees ("scrutinizers") which, for security reasons, were not allowed to report details of the findings internally. SWIFT also mentioned that it is overseen by a senior committee drawn from the G-10 central banks and that SWIFT has informed the overseers of this matter.

---

[33] Opinion Belgian DPA, cf. footnote 8.

Although the control measures put in place by SWIFT may contribute to enhance the security of the data processing activities, the Working Party strongly insists that no other mechanism provided for by data controllers can replace the control of data processing activities by a public independent supervisory authority as required by Article 28 of the Directive. In any case, the oversight group set up by the G-10 central banks declared itself incompetent to examine any question relating to the protection of personal data.

As a result, the Working Party condemns the fact that the existing mechanisms for independent control by the public supervisory authorities of personal data processing have been circumvented for the personal data processed via the SWIFTNet FIN service.

4.6. Transborder data flows (Articles 25 and 26 of the Directive)

Articles 25 and 26 of the Directive apply where personal data are transferred to a third country. Any transfer of data generated within EU territory that is to be used outside EU territory has to be subject to an adequacy assessment pursuant to the Directive. Furthermore, the provisions of the Directive relating to transfers of personal data to third countries cannot be applied separately from other provisions of the Directive. As explicitly mentioned in Article 25(1), these provisions apply "without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive". This means that regardless of the provisions relied upon for the purpose of data transfer to a third country, other relevant provisions of the Directive need to be respected[34].

The normal functioning of the SWIFTNet FIN service includes a continuous and massive transborder data flow, due to the location of the SWIFT operating centres. The SWIFT operating centres are not separate legal entities, but branches ("*succursales*") of the cooperative company established under Belgian law. The store-and-forward capability of the two SWIFT operating centres in Europe and in the US operates as follows: The messages are decrypted automatically in the operating centres to store and forward the information in a few milliseconds. This "store-and-forward" process is intended to validate (control the correctness or the presence of letters/numbers in the mandatory message fields) the information (for instance make sure that the correct currency code of the transfer is filled in, e.g. "EUR") on the basis of contents that is standardized. During this process, the information is also stored for 124 days in both operating centres for security (back-up) reasons which then act as perfect "mirrors". This ensures that the data storage is parallel and the data are identical.

For SWIFT to lawfully process and mirror personal data in the US it needs first for these data to be transferred from the EU pursuant to Belgian law adopted in accordance with the Directive, in particular Articles 25 and 26 on the transfer of personal data to third countries. The transfers by SWIFT to the United States therefore have to be considered taking account of two elements: firstly, the commercial processing and mirroring of personal data by SWIFT Belgium to its operating centre in the US, and secondly, the processing of the data for the further purpose by the UST as agreed to by SWIFT.

---

[34] Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. WP 114.

4.6.1. Adequate data protection (Article 25 (1) of the Directive)

According to Article 25 (2) of the Directive, the adequacy of the level of protection afforded by a third country "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

Taking into account the above criteria and applying the principles defined in Working Document WP12[35], the Working Party finds that in the USA currently only the "Safe Harbour" scheme provides for an adequate level of protection for data transfers from the EU to US organisations having joined this scheme. However, it does not cover financial services[36],.

Therefore, as a Belgian legal entity, SWIFT could not rely on Article 25 of the Directive for the processing and mirroring in the US operations centre.

4.6.2. Adequate safeguards put in place by recipient (Article 26 (2) of the Directive)

Under Article 26(2) of the Directive a Member State may also authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection where the data controller offers "*adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights*". The end of Article 26(2) also states that these safeguards "*may in particular result from appropriate contractual clauses*". To facilitate the use of contractual clauses, the European Commission has issued three decisions on standard contractual clauses, two of which regulate transfers from a data controller to a data controller while the third regulates transfers from a data controller to a processor[37]. In addition, apart from the possibility of using contractual clauses to provide such sufficient safeguards, since 2003 the Article 29 Working Party has been working actively on the possibility of multinational groups using "binding corporate rules" for the same purpose[38].

---

35 "Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive", adopted by the Working Party on 24 July 1998; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.

36 cf. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

37 As regards transfers from a data controller to a data controller, the Commission issued a first set of standard contractual clauses on 15 June 2001; it subsequently amended this decision in order to annex a new set of alternative clauses (decision of 27 December 2004). With regard to transfers from a data controller to a processor, the Commission issued a set of standard contractual clauses on 27 December 2001. All these clauses are available on the following website: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

38 Cf. Working document WP 74, "Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers"

However, in this case, SWIFT has not made use of these possibilities for its processing and mirroring in the US operating centre.[39]

4.6.3. Derogations (Article 26 of the Directive)

Article 26(1) of the Directive states that transfers of personal data to a third country which does not ensure an adequate level of protection may take place if one of the following conditions listed under (a) to (f) is met. As previously indicated by the Working Party in its working document WP12[40] mentioned above, the interpretation of Article 26(1) must necessarily be strict.

In this respect, the Working Party emphasises that this logic is the same as that of the additional protocol to Council of Europe Convention 108. The report on this protocol states that "the parties have discretion to determine derogations from the principle of an adequate level of protection. The relevant domestic provisions must nevertheless respect the principle inherent in European law that clauses making exceptions are interpreted restrictively so that the exception does not become the rule".[41]

The possible derogations in this case are as follows:

4.6.3.1. Consent of the data subject (Article 26 (1) (a) of the Directive)

For this derogation to be lawfully invoked, the data subject must give his/her consent unambiguously to the proposed transfer. As already indicated in the Working Party's previous working document WP 12 this consent, whatever the circumstances in which it is given, must be a freely given, specific and informed indication of the data subject's wishes, as defined in Article 2(h) of the Directive.[42] The data subject must be informed of the transfer to a third country without an adequate level of protection or without having put in place the appropriate safeguards and can then decide whether he will run the associated risk or not.

SWIFT has not obtained the unambiguous consent of the data subjects for the processing and mirroring in the US operating centre and therefore cannot rely on Article 26 (1) (a) of the Directive.

4.6.3.2. Transfer is necessary for performance of a contract between the data subject and the controller or for the implementation of

---

adopted by the Working Party on 3 June 2003 and further complementary documents WP107 and WP108.

39 In any case, if SWIFT were to make use of these possibilities, the Article 29 Working Party recalls that for any onward data transfer derogations from the applicable data protection law may not go beyond the restrictions necessary in a democratic society.

40 Cf. footnote 35, above.

41 Cf. report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data, Article 2(2)(a); this document can be accessed at:

http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

42 Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. WP 114.

precontractual measures taken in response to the data subject's request (Article 26 (1) (b) of the Directive)

This exception means that the data transferred must be truly necessary to the purpose of the performance of this contract or of these precontractual measures. For this reason, the Working Party takes the view that this condition could not be applied to transfers of data by SWIFT to the US operating center, as SWIFT does not have a direct contractual relationship with the individual. Also, this derogation cannot be applied to transfers of additional information not necessary for the purpose of the transfer, or transfers for a purpose other than the performance of the contract. More generally, the derogations of Article 26(1)(b) to (e) only allow that the data which are necessary for the purpose of the transfer may be transferred on the basis of the individual derogations; for additional data, other means of adducing adequacy should be met.

4.6.3.3. Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party (Article 26 (1) (c) of the Directive)

Likewise the derogation under Article 26(1)(b), a transfer of data to a third country which does not ensure adequate protection cannot be deemed to fall within the exception contained in Article 26(1)(c) unless it can be considered to be truly "necessary for the conclusion or performance of a contract between the data controller and a third party, in the interest of the data subject", and pass the corresponding "necessity test". This test requires a close and substantial connection between the data subject's interest and the purposes of the contract.[43]

The Working Party takes the view that this condition may not be applied to transfers of data by SWIFT to the US operating centre.

4.6.3.4. Transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (Article 26 (1) (d) of the Directive)

SWIFT stated that the mirroring of processing data to the operations centres was considered as a critical element in the global financial system and that this mirroring of processing had been proposed by the overseers (G-10 central banks) for security reasons and reliability, and that SWIFT infrastructure would be considered critical for the global financial industry. SWIFT argues that this ground would justify the transfer on the basis of Art. 26(1)(d) of the Directive.

The Working Party cannot follow this interpretation. Even if it would be established that international mirroring of the processing (on a different continent other than Europe) would be "necessary or legally required on important public interest grounds" in the meaning of Article 26(1)(d) of the Directive, 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[44] or Canada[45], that,

---

[43] Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. WP 114

[44] Commission Decision C(2003) 1731 of 30 June 2003; OJ L 168, 5.7.2003.

according to European Commission Decisions, are considered as satisfying the requirements of the Directive. The "mirroring" in a non-EU country without an adequate level of data protection was is not necessary and cannot be justified by Article 26(1)(d).

Furthermore, personal data, collected and processed via the SWIFT network for international money transfers using the BIC or "SWIFT" code, and mirrored in the US, were provided to the UST since the end of 2001 on the basis of subpoenas under US law.

The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation, detection and prosecution of money laundering and the financing of terrorism and has been subject to regulation under EU law[46].

The Working Party recognizes that the fight against terrorism constitutes a legitimate purpose of the democratic societies in the interest of the safety of the state and that to this end measures can be taken which interfere with the fundamental right to personal data protection. The Working Party recalls its full commitment in this respect. It also considers that international instruments do provide for an appropriate legal framework enabling international cooperation. To this end, the Working Party is of the opinion that the possibilities already offered by current international forms of cooperation set up in respect of the fight against terrorism and terrorism investigation should be exploited while ensuring the required level of protection of fundamental rights.

The Working Party notes nevertheless that Article 26 (1)(d) of the Directive does not apply either as the transfer is not necessary or legally required on important public interest grounds of a EU Member State (Belgium). On this point the drafters of the Directive clearly did envisage that only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in this connection. Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in the Directive.

4.6.3.5. Transfer is necessary in order to protect the vital interests of the data subject (Article 26 (1) (e) of the Directive)

This exception applies to transfers that must relate to the individual interest of the data subject and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, this exception could not be used to justify transferring personal medical data for a purpose such as general medical research.[47]

SWIFT has not claimed that the transfer is necessary in order to protect the vital interests of the data subjects for the processing and mirroring in the US operating centre. The

---

45 Commission Decision 2002/2/EC of 20.12.2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act; O.J. L 2/13 of 4.1.2002.

46 E.g. Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, adopted on 8 November 2006, not yet published; initial Commission Proposal COM (2005) 343.

47 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

Working Party considers that in any case this exception is irrelevant here. Article 26 (1) (e) of the Directive cannot be relied upon.

4.6.4. Findings

SWIFT may have relied on Article 26 (2) of the Directive for making a legal transfer of personal data to its operating centre in the US. However, SWIFT decided to transfer personal data without having complied with the legal requirements under Belgian law for such international data transfers.

SWIFT cannot rely on any of the other exceptions of Article 26 of the Directive.

As for the processing and mirroring in the US, even the commercial processing and mirroring did not take place legally. The continuing processing and mirroring, considering its further incompatible purpose and its large scale does not fall within the boundaries of what is necessary in a democratic society and further prevents SWIFT from transferring the personal data to the US.

5. CONCLUSIONS:

On that basis, the Working Party is of the opinion that:

5.1. The EU Data Protection Directive 95/46/EC is applicable to the exchange of personal data via the SWIFTNet FIN service;

5.2. SWIFT and the financial institutions bear joint responsibility in light of the Directive for the processing of personal data via the SWIFTNet FIN service, with SWIFT bearing primary responsibility and financial institutions bearing some responsibility for the processing of their clients' personal data.

5.3. SWIFT and the financial institutions in the EU have failed to respect the provisions of the Directive:

5.3.1. *SWIFT*: As far as the processing and mirroring of personal data in the framework of the SWIFTNet FIN service is concerned, SWIFT as a data controller must comply with its obligations under the Directive, amongst which are the duty to provide information, the requirement to notify the processing, the obligation to provide an appropriate level of protection in order to meet the requirements for international transfers of personal data;

5.3.2. *Financial institutions*: The financial institutions in the EU as data controllers have the legal obligation to make sure that SWIFT fully complies with the law, in particular data protection law, in order to ensure protection of their clients. The financial institutions are responsible for having sufficient knowledge of the different payment systems and their technical and legal characteristics and risks. If financial institutions did not strive (sufficiently) to obtain such knowledge, they would accept substantial legal and client risks in breach of their fundamental duty of care. In particular, if some services such as the SWIFTNet FIN service involve massive

transfers to countries without adequate data protection in the light of the Directive or if it is likely that such transfers would pose specific privacy concerns or risks, the Working Party is of the opinion that it is essential that the individual clients of the financial institutions are informed by the financial institutions, as their providers of professional services, in accordance with the transparency requirements of the Directive.

5.4. The Working Party is of the opinion that the lack of transparency and adequate and effective control mechanisms that surrounds the whole process of transfer of personal data first to the US, and then to the UST represents a serious breach in light of the Directive. In addition, the guarantees for the transfer of data to a third country as defined by the Directive and the principles of proportionality and necessity are violated.

As far as the communication of personal data to the UST is concerned, the Working Party is of the opinion that the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years without effective legal grounds and without the possibility of independent control by public data protection supervisory authorities constitutes a violation of fundamental European principles as regards data protection and is not in accordance with Belgian and European law. An existing international framework is already available with regard to the fight against terrorism. The possibilities already offered there should be exploited while ensuring the required level of protection of fundamental rights.

5.5. The Working Party recalls once again[48] the commitment of democratic societies to ensure respect for the fundamental rights and freedoms of the individual. The individual's right to protection of personal data forms part of these fundamental rights and freedoms[49]. The Community Directives on the protection of personal data (Directives 95/46/EC and 2002/58/EC) form part of this commitment[50]. These Directives aim to ensure respect for fundamental rights and freedoms, in particular, the right to privacy with regard to the processing of personal data and to contribute to the respect of the rights protected by Article 8 of the European Convention on Human Rights, and Article 8 of the EU Charter of Fundamental Rights. In all these instruments, exceptions to combat crime are provided for but have to respect specific conditions.

---

48 Article 29 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm .

49 See in particular Art. 8 Charter of Fundamental Rights of the European Union as well as case-law of the European Court of Human Rights in the affairs "Aman" of 16 February 2000 and "Rotaru" of 4 May 2000.

50 See recitals 1, 2, 10 and 11 of Directive 95/46/EC.

6. IMMEDIATE ACTIONS TO BE TAKEN TO IMPROVE THE CURRENT SITUATION:

In view of the above, the Working Party therefore calls for the following immediate actions to be taken to improve the current situation:

6.1. **Cessation of infringements:** SWIFT and the financial institutions shall comply with their legal obligations under national and European law. This includes taking steps to ensure that any transfers of personal data are in line with the law. In case of non-compliance, data controllers can expect to be subject to sanctions imposed by the competent authorities under the Directive and national law, in order to enforce compliance.

6.2. **Return to lawful data processing:** The Article 29 Working Party calls upon SWIFT and the financial institutions to immediately take measures in order to remedy the currently illegal state of affairs, and to return to a situation where international money transfers may be made in full compliance with data protection law. The Working Party welcomes the fact that some data protection authorities are already urging the financial institutions to find a solution without delay.

6.3. **Actions as regards SWIFT:** For all its data processing activities, SWIFT as a controller must take the necessary measures to comply with its obligations under Belgian data protection law implementing the Directive.

6.4. **Actions as regards Central Banks:** The present situation calls for a clarification of the oversight on SWIFT. The Working Party recommends that appropriate solutions are found in order to bring compliance in particular with data protection rules clearly within the scope of the oversight, without prejudice to the powers of national data protection supervisory authorities, as well as to ensure that relevant authorities are duly and timely informed where necessary. The Working Party considers that the lack of compliance with data protection legislation may actually hamper consumers' trust in their banks and might thus affect also the financial stability of the payment system (reputation risk). Legal obstacles such as professional secrecy obligations of the overseers that could be used as argument to limit the effective control by the independent data protection authorities, should not be relied upon in a case of possible violation of constitutional or human rights.

6.5. **Actions as regards Financial Institutions:** All financial institutions in the EU using the SWIFTNet Fin service including the Central Banks have to make sure that according to Articles 10 and 11 of the EU Directive 95/46/EC their clients are properly informed about how their personal data are processed and which rights the data subjects have. They also have to give information about the fact that US authorities might have access to such data. Data protection supervisory authorities will enforce these requirements in order to guarantee that they are met by all financial institutions on a European level and they will cooperate on harmonized information notices. The Article 29 Working Party recalls in this connection its opinion adopted

on harmonized information provisions[51]. It also seems appropriate for financial institutions and Central Banks to consider alternative technical solutions to the procedures that are currently used, in accordance with the principles of the Directive.

The Working Party also stresses the following:

6.6. **Preservation of our fundamental values in the fight against crime:** The Working Party recalls that any measures taken in the fight against crime and terrorism should not and must not reduce standards of protection of fundamental rights which characterise democratic societies. A key element of the fight against terrorism involves ensuring the preservation of the fundamental rights which are the basis of democratic societies and the very values that those advocating the use of violence seek to destroy.

6.7. **Global data protection principles:** The Working Party considers it essential that principles for the protection of personal data, including control by independent supervisory authorities, are fully respected in any framework of global systems of exchange of information.

The Article 29 Working Party will follow-up and monitor all of the above.

Done at Brussels, on 22 November 2006

For the Working Party
The Chairman
Peter Schaar

[51] Article 29 Working Party "Opinion on More Harmonised Information Provisions", 25 November 2004. WP 100; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.