ROYAUME DE BELGIQUE

COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

Adresse : Rue Haute, 139, B-1000 Bruxelles
Tél. : +32(0)2/213.85.40 E-mail : commission@privacycommission.be
Fax : +32(0)2/213.85.65 Site Internet : http://www.privacycommission.be

NON-OFFICIAL AND TEMPORARY TRANSLATION as of 29092006

This version is made by the Secretariat of the Commission and is intended for convenience purpose only. This text is not formally approved by the collegial body of the Commission. Only the Dutch and French texts should be relied upon as the official and approved versions of the opinion.

Opinion No. 37 / 2006 of 27 September 2006

O. Ref.: SA2 / A / 2006 / 037

CONCERNING: Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas

The Data Protection Commission;

Considering the Directive 95/46/EG of the European Parliament and the Council dd. 24th October on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("95/46/EG Directive")

Considering the law of 8th December 1992 regarding the protection of privacy with regard to automatic processing of personal data ("DPL"), especially article 29 § 1;

Considering the request for advice by the Council for Information and Security dd. 6th July 2006, received by the Commission on 19th July 2006;

Considering the correspondence with SWIFT;

Considering the report of Mr. De Schutter;

Gives the following advice on 27th September 2006:

A. INTRODUCTION

On 19th July 2006 the Commission received a request for advice from the Council for Information and Security on "whether, in the framework of the "SWIFT" case, there is question of violation of Belgian legislation, more specifically a violation of the DPL. The Commission was also asked to provide the Commission with all the elements which could be useful in the fulfilling of its mandate.

During its session of 5th July 2006, the Commission had already made the decision to officially start an investigation into this case on grounds of article 32 § 1 DPL[1], regarding the processing of personal data under the responsibility of SWIFT, a cooperative society under Belgian law, with headquarters in Belgium and with limited liability (CSLR or "CVBA" in Dutch / "SCRL" in French). This as a result of various news articles which were published[2] at the end of June regarding the role played by SWIFT in the transfer of personal data to the US Department of the Treasury (UST), more specifically the Office of Foreign Assets Control (OFAC).

Finally, on 28th June 2006, the Commission received a public complaint formulated by the "privacy International" organisation which was sent to the data protection authorities and regulators of 33 countries in relation to the afore-mentioned news articles.

The investigation by the Commission focused exclusively on the afore-mentioned issue and did not relate to the processing of personal data typical of the normal administrative or management activities of a company (personnel administration, client management, a.o.) The Commission established that SWIFT did make the necessary notifications to CBPL according to the DPL. Attention was focused on the data flow via the "SWIFTNet FIN" service and the communication to the UST of data generated via this service. The Commission has no knowledge of any other transfer of data to the UST with regard to other services.

In the preparation of its opinion, the Commission relied on SWIFT information which was in the public domain[3], documents to which SWIFT granted the Commission access (in application of art. 31 § 1 DPL), elements from repeated inquiries[4] and information obtained during consultations with SWIFT managers (general counsel, the CEO, the responsible for the audit, legal department, legal advisors) dd. 23rd August, 31st August (on-site investigation) and finally elements from the internal meetings of the Commission dd. 6th and 27th September 2006. Parallel thereto, a written inquiry was made to the National Bank of Belgium in a letter dated 10th August 2006.

---

[1] In advice dd. 13th November 1996 regarding the preliminary draft of the law in adaptation of the law of 8th December 1992 to the 95/46/EG Directive, one can read that the Commission deems itself competent to carry out on-site checks at its own initiative or, upon a complaint or, on grounds of the disclosure of information of a very sensitive nature.

[2] In particular The New York Times ("bank Data is sifted by US in secret to block terror" dd. 22nd June 2006), (www.nytimes.com), The International Herald tribune ("oversight on records defended" dd. 25th June 2006); , Los Angeles Times ("secret US Program tracks global bank transfers" dd. 23rd June 2006) and subsequent world wide reactions from the press.

[3] Especially the information on the SWIFT website www.swift.com and other printed information

[4] CBPL correspondence dd. 7th July and reply from SWIFT dd. 28th July
CBPL correspondence dd. 8th September and reply from SWIFT dd. 14th September 2006

Also to be mentioned is the fact that the issue of the onward transfer to the UST is as well under discussion within the European Union[5] and with a number of data protection authorities ("DPL's") inside and outside Europe (Germany, Italy, France, Canada, Australia, a.o.).
The Commission consulted on this issue the European Group of data protection Commissioners; founded on the basis of article 29 of the 95/46/EG Directive (here-after called the "art 29 Working Party"). The art. 29 Working Party declared on 26 September 2006[6] that they consider it a "priority to safeguard European data protection rights". The Group also did express immediate concerns about the lack of transparency which has surrounded the arrangements with the UST.

B. FACTS AND LEGAL CONTEXT

B.1. SWIFT

SWIFT is a cooperative limited-liability company governed by Belgian law, with registered office at La Hulpe (Belgium). SWIFT supplies its customers, i.e. financial institutions, automated, standardized services ("messaging services") and interface software aimed at transmitting financial messages between financial institutions world wide. SWIFT itself is not a bank , nor any other kind of financial institution.
Approximately 7,800 financial institutions are a member of SWIFT. In relation to its service, SWIFT does not hold exclusivity. Financial institutions can have their payment transfers processed through different providers and means (VPN providers, internet, fax, banks' networks, VISA, etc. …).Apart from sales offices in various countries, SWIFT has two operation centres (OC) located in SWIFT branches, one in Europe and one in the United States. In these OC's , as part of the SWIFTNet FIN service, all messages processed by SWIFT are stored, in mirror, during 124 days, in order to be able to act as a "back-up recovery tool" for a customer in case of disputes between financial institutions or loss of t data. After this period , the data is erased.

B.1. 1. Description of the data flow and data which are processed via the SWIFTNet FIN service.

The data carried by SWIFT in the cope of the SWIFTNet FIN service concerns the transmittal of messages concerning the financial transactions between financial institutions. It is noteworthy that SWIFT therefore only deals with professional customers and does not sustain any direct contractual relationships with customers (physical persons) of financial institutions, who would reques or receive a financial transaction on or through their accounts. Furthermore, SWIFT only supplies services to financial institutions that have signed a prior contractual agreement. This contractual agreement is known to the financial institutions calling upon the SWIFTNet FIN service and consists among others of the SWIFT by-laws ("by-laws"), the general terms and conditions, the specific service related documentation (all included in the "SWIFT User Handbook") and the SWIFT data retrieval policy. They are supplemented with SWIFT's compliance policy[7] .

[5] In the protection of persons group regarding personal data processing, founded on grounds of article 29 of the 95/46/EG Directive, hereafter called "Group 29"
[6] See the press statement on
http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf
[7] The SWIFT declaration on compliance can be found on its website www.swift.com.

In that respect, the electronically transmitted messages can be compared with an "envelop" and a "letter", whereby the "envelop" (or the header of the message) contains information on the sender, its BIC-code[8], the identification of the receiving bank and finally the date and time of the message. The "letter" (content of the envelop), i.e. the actual message, is encrypted through PKI encryption and contains information which is entered via standardized fields. If it concerns a message related to a bank's customer payment[9], this information contains at the least the amount of the transaction, the currency, the value date, the beneficiary's name, the beneficiary's financial institution, the customer requesting the financial transaction and the customer's financial institution requesting the transaction. Payment related messages can, however, also contain other information, such as reference numbers for payments and (for some types of messages) "unstructured (free format) text" .

The itinerary of a cross-border payment message sent via the SWIFTNet FIN service is as follows: (the first and fourth steps are outside the SWIFT operation).

1. An individual payment order from an ordering customer (an individual or a company) to its bank ("originator's bank"). Unless the originator's bank or the instructing customer chooses an alternative service or solution other than SWIFT, the originator's bank composes a standardized and encrypted SWIFT message;
2. The originator's bank sends the standardized SWIFT message using the SWIFTNet FIN service, or chooses an alternative way or solution other than SWIFT. The message is sent thereafter either to a correspondent bank abroad, or directly to the bank of the beneficiary (if the originating bank has direct correspondence relations with the bank of the beneficiary);
3. the correspondent bank sends the same message through the SWIFT network to beneficiary's bank;
4. the beneficiary's bank informs the beneficiary that its payment has arrived and credits the beneficiary's account accordingly.

In this , SWIFT acts as the carrier of the standardized message in a closed envelop. The messaging service includes, at the operations centres' level, a formal validation of its content, in particular of the presence or correct content of the data filled out in the provided fields (e.g. has the addressee's bank been filledin, has the currency been indicated,…). This does require a moment of decryption of the message's content, including personal data, which is entirely automated. As part of the messaging service the messages are also stored at the operations centres in Europe and the US for the above-mentioned period of 124 days.

[8] BIC (Bank Identifier Code) is an international identification code (sometimes also called swift-code), which allows for the identification of every individual bank.
[9] A client transfer is one of nine categories of SWIFT messages.

B.2. Subpoenas

After the attacks of September 2001, the UST has addressed multiple 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 in the aftermath of the attacks of 11th September 2001.

Before 2001, SWIFT had also been subject to some judicial or administrative subpoenas, but these were not complied with either for reasons of timeframe (after 124 days) or, because SWIFT could argue that the authority could more easily demand the data from the sending or receiving bank, or because SWIFT has no research tool in its operating centre for queries on a name basis. The UST subpoenas are of an entirely different nature and can be qualified as ***non individualised mass requests ("Rasterfandung" "carpetsweeping" technique)*** in a first phase (cf. infra). The scope of the subpoenas 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 an x number of countries and jurisdictions, on that date, or from … to … ranging from one to several weeks, within and outside the US,…) It concerns messages of inter-bank transactions within the U.S., to or from the U.S., as well as messages from outside the US, such as e.g. within the EU.

It appears that the UST departs from a broad **definition of "terrorism"** such as "dealing with terrorist attacks against the US which that took place on September 11, 2001 and with a global network of terrorist cells that could pose a threat to US citizens,persons, USproperty and interests, domestic or abroad". It further appears from the negotiations that SWIFT has agreed a second (conventional) definition of terrorism with the UST which reads as follows: "an activity that (i) involves a violent act or an act dangerous to human life, property, or infrastructure; and (ii) appears to be intended (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking. This includes, but is not limited to, activities engaged in by known terrorist organizations, but excludes activities of recognized governments[10]." The Commission notes that in this conventional definition any reference to the US has been omitted.

It appears from the verifications of the Commission that in the collection process, a distinction **was made between two levels**; on the one hand, the storage in a black box of messages delivered as a result of the subpoenas, and on the other hand, the actual UST consultation of the messages in the black box on the basis of searches. Both steps are described hereafter.

Any **messages subjected to subpoenas** ("subpoenaed messages") are delivered by the SWIFT operations centre in the US to the UST where they are kept in a so-called **black box** ("black box" or "production database") which is retained at UST facilities.

[10] (the definition in English is placed in this footnote in the official Dutch and French Version)

An automatic decryption takes place in the black box by means of a tool (search software) which was designed and is owned by the UST, whereupon the UST can perform searches by name. This search software, which is not available to SWIFT, examines whether certain predetermined names of suspects appear in the messages[11]. It was agreed between SWIFT and the UST that the UST can only make pointed requests relating to targeted investigations into terrorist activities.

Further to a formal request by the Commission, SWIFT did not provide any exact figures on the number of messages which could be contained in the black box. SWIFT provided the reason that the UST deems this information of importance to national security. It was also disclosed that this information could only be released by the UST upon implementation of the appropriate security procedures with Belgian officials with the appropriate security clearance.

Nevertheless, it can be deducted from the general scope of the subpoenas and the average volume of the number of messages processed on a daily basis by the SWIFTNet FIN service that the number of subpoenaed messages in the black box must be enormously high.SWIFT confirmed in a letter of 14 September 2006 that the UST has "the full right under US law to subpoena SWIFT US branch to provide all SWIFT messages." This means that, for the year 2005 alone, a total number of 2,518,290,000 SWIFTNet Fin messages can be subject to the subpoena[12].

B.3. Reaction from SWIFT to the subpoenas

SWIFT obtained a number of guarantees and protection mechanisms from the UST. The principles thereof were formally documented in correspondence between SWIFT and the UST.

B.3.1. Negotiations with UST

SWIFT decided not to challenge the subpoenas, issued against SWIFT's "branch" in the US and not against SWIFT CSLR, before the American court, but instead to immediately negotiate with the UST to obtain clear guarantees. SWIFT stresses that thanks to these negotiations it obtained a unique level of protection with regard to the data transmitted.

As far as the Commission could verify on the basis of the documents presented, the first documented agreements related to the appointment of an external auditor (Booz, Allen & Hamilton) and the characteristics of the auditing process as of August 2002. On 15 September 2003, SWIFT received a "comfort letter" from the UST in which the UST offered SWIFT its support, should third parties such as governments of other countries question compliance with the UST subpoenas. As per 14 April 2004, a number of significant guarantees were inventoried, some of which had been negotiated from the beginning of the process. They concerned an agreement of the definition of terrorism and of the criteria for the search orders and the retrievals on 27th February 2004 and agreements concerning the maximum confidentiality of the data retrieved, the control of SWIFT over the search criteria and on the collections. Also, SWIFT received the guarantee that the original source of the information (SWIFT) would be kept confidential by the UST.

[11] As confirmed to SWIFT by the UST on 1st August 2002

[12] A figure mentioned in the same letter of SWIFT of 14 September 2006. One can also start from the average and normal daily message traffic via SWIFTNet FIN which lies somewhere in between 6.9 million (2005) and 11 million messages per day (start of 2006) which, in its totality, can be subjected to subpoenas.

Summarized the guarantees as agreed between the UST and SWIFT concerned the following:

- the UST does not have any access to the SWIFT system itself and the data stored therein;
- only data related to terrorism investigations can be retrieved;
- the search orders in the black box are only possible on the basis of specific, targeted investigation files concerning terrorist activities;
- A continuous audit by the American auditor Booz, Allen & Hamilton was provided for as of the middle of 2002. This concerns end-to-end audits of the UST's system to provide SWIFT with additional assurance that the system was secure (checking the conformity with ISO standards on security), that the purpose was limited to terrorism investigations, that the scrutinizers (cf. hereafter) had access to everything the UST analysts were inquiring and to force continuing improvements to the system;
- Two employees of SWIFT ("scrutinizers") received a security clearance to be present at the extraction of the data by the UST. They review the justification for each UST extraction on a regular basis, initially via statistical sampling, later at the 100% level. They only report to SWIFT's management in relation to the compliance with the extraction principles, not on the details of specific extractions.

- The UST black box remains subject to the control of the "scrutinizers" by means of a 24-hour access, real-time monitoring and the possibility to block the search orders, even as of the moment the black box is placed on a physically secured location of the American government;
- In the event that UST were to seek a court order requiring SWIFT to comply with a subpoena, UST agreed not to cite as precedent or rely upon such fact, and SWIFT reserved all of its defenses to any such action;
- The possibility was provided for SWIFT to retrieve all non-retrieved messages from the black box, albeit under the obligation to store these data for as long as the possibility exists that a subpoena be ordered in respect of these data;
- Strict confidentiality standards were determined.

B.3.2. Information to the Supervisors

At first, only the legal validity of the subpoenas was verified by the general counsel and external advisors. Decisions on the compliance with subpoenas were made by SWIFT's CEO, the Board of Directors and the Audit and Finance Committee or "AFC". The Board of Directors received a short clarification about the subpoena from the Chairman of the Audit and Finance Committee. In March 2002, the Board of Directors was given a presentation on this subject and had an in depth discussion regarding this topic., Further reporting has since been given periodically.
SWIFT also informed the "Senior level oversight Group" (G–10), amongst which the National Bank of Belgium. The Commission asked the National Bank of Belgium ("NBB") for information relating to the oversight powers of the NBB by way of a letter of 10 August 2006. . The NBB confirmed in its reply of 29 August 2006 that "the NBB had been informed by SWIFT in February 2002,in its capacity of "overseer", of the existence of an American subpoena issued against SWIFT's branch in the United States."

The NBB considers that it is not competent to issue an opinion on SWIFT's compliance with the consecutive UST subpoenas. This point of view is also shared by the G-10.

C. APPLICABILITY OF THE DPL

It must be checked whether the DPL applies to SWIFT as manager of the SWIFTNet Fin system, in the capacity of "data controller" or in the capacity of "processor".

C.1. Territorial scope

The DPL applies to *"the processing of personal data carried out in the context of the effective and actual activities of a permanent establishment of the data controller on Belgian territory (...)" (article 3bis, 1° DPL)*

The registered office and head office of SWIFT are located in Belgium and the company has a Belgian company number, i.e. 413330856. Therefore, there is no doubt that there are "*effective and actual activities" and a "permanent establishment on Belgian territory"* apart from the question whether SWIFT is the data controller[13], a question which will be dealt with hereafter.

SWIFT referred to the fact that the operations centre in the US is not a separate legal entity and that (within the normal internal processing of data of the SWIFTNet FIN service) there is no question of any communication of data to an external company outside the EU.

From a company law point of view, SWIFT concludes on this basis that the processing of data was always subject to therules applicable to the Belgian company as the operations centre could be legally identified with SWIFT CSLR. It concludes on this basis that the protection under Belgian law is also applicable to its operations centre in the US. Even though SWIFT used this company law argument to question the application of articles 21 and 22 of the DPL (cf. infra), the Commission notes that this argument of company law can additionally confirm that the processing of personal data is subjected to Belgian law, including the DPL.

C.2. Substantive scope

From the description of the data flow and the data processed by the SWIFTNet Fin service (cf. supra item B.1.), it is obvious that this is indeed a matter of "processing" of "personal data" in the sense of article 1 §§1 and 2 of the DPL. The financial messages which are processed[14] and stored in the framework of the SWIFTNet FIN service do contain data on physical persons such as the identity of the beneficiary and the identity of the client of financial institutions such as payment instructions.

Finally, it must be noted that article 10.10 of SWIFT's general terms and conditions provides that the Belgian law is applicable to the provisions and conditions concerning the supply and use of the SWIFT services and products. This includes of course the Belgian legislation on the protection of personal data and the DPL.

[13] For the analysis on the responsibility of SWIFT, cf. hereafter.

[14] According to article 1 § 2 DPL "processing" is the collection, extraction, consultation, use, disclosure by means of transmission, distribution or any other form of making personal data available as well as the coordination of personal data.

D. OPINION ON WHETHER SWIFT, THE FINANCIAL INSTITUTIONS AND THE NATIONAL BANK OF BELGIUM ARE DATA CONTROLLERS OR PROCESSORS

In response to the question from the Council for Information and Security, the role of SWIFT, the clients of SWIFT (here-after called the "financial institutions") and the National Bank of Belgium must be examined in the light of the DPL.

The question is whether SWIFT, the financial institutions or the National Bank of Belgium are to be considered as data controllers or as processors. The responsibility for the compliance with the DPLL lies in principle with the data controller. Article 1 § 4 of the DPL defines the data controller as "(...) *the legal person (…) that, alone or jointly with others determines the purposes and means of the processing of personal data.* The processor, on the other hand is the "*physical person, legal person, factual association or public authority (...)that processes personal data on behalf of the data controller, except for the persons who are, under the direct authority of the controller, authorised to process the data*". The distinction between both qualifications has very important consequences regarding the compliance with the DPLDPL: underDPLDPL this Act , the processor has in principle a limited liability and the persons concerned can in principle only assert their rights on the data controller.

The legal definition in article 1 § 4 DPL is **of imperative law** and it cannot be deviated from by means of contractual agreements.

While determining who actually is data controller, the DPL provides in essence a **functional criterion**. In other words, the question is who had 'a hold' on the processing of personal data via their SWIFTNet FIN service or who could de facto make the crucial decision on the purposes and the means of the processing. In this respect, formal criteria such as the contractual description of the services or the capacity of the contracting parties are useful , but a priori not a deciding factor.

In order to make a correct judgment on any possible classification of afore-mentioned actors, it must be kept in mind which are the purposes and therefore the types of processing targeted. The Commission considers it necessary to make a distinction between the following types of processing: on the one hand, the functioning of the SWIFTNet FIN service and, on the other hand, the execution of international payment instructions involving the SWIFTNet FIN service.

D.1. The processing of data in the framework of the SWIFTNet FIN service

SWIFT systematically stated that with regard to the messaging service, it is not the data controller but merely a processor. In support, SWIFT used a number of arguments during its contacts with the Commission which can be summarized as follows:

- SWIFT compares itself to a service provider of telecommunication or electronic mail who is normally assumed not to be the data controller responsible for processing but merely the processor[15];

[15] Consideration 47 of the 95/46/EG Directive states that "when a message containing personal data is transferred by telecommunication or electronic mail service, which has as sole function to transmit this type of messages, it is the sender of the message, and not the service provider, who will normally be deemed to be the controller of the personal data contained in the message; the persons offering this service will normally be deemed data controller in relation to the additional personal data required to provide the service.

- SWIFT states that in its contractual agreements with the financial institutions[16], the identification of SWIFT as processor is laid down;
- SWIFT argues that, as a processor, it has "a normal margin for manoeuvre" in determining the organisation of its service, in particular with regard to technical and organizational measures required with regard to processing;
- SWIFT states that it provides services in a "business- to business" environment in which it does not have any direct contact or contractual relationship with the clients of the financial institutions, including any natural persons;
- SWIFT finally states that it did not establish or develop any search capacity to look up personal data which might be mentioned in the messages handled by them.

Considering the functional definition of the data controller under the DPL, the Commission considers the **context in which the processing is performed** (cooperative society with limited liability) and **the knowledge of the exact position of the financial institutions and the management of SWIFT** CSLR crucial in order to establish an exact classification regarding the normal processing of data within the SWIFTNet FIN service.

The comparison of SWIFT CSLR to a normal service provider of telecommunication and electronic mail is a formal argument and seems inadequate. This formal comparison implies that SWIFT would have a comparable position to any random telecommunication company which offers a VPN on an international level for the exchange of financial messages. In reality, SWIFT seems to operate a more complex modus operandi and service format which emanates from an **international cooperative network with strong central management** vis-à-vis the 7,800 financial institutions availing of its services. The running and workings of such networks differ fundamentally from the simple service concept in which one professional provider processes personal data in respect of a professional or non-professional third party. The assessment of the classification "data controller" or "processor" is in this context delicate. In case of imbrications of various actors it is important to determine the role and the responsible parties for every entity.

Due to its international and non-transparent nature the normal processing within the SWIFTNet FIN service seem quite opaque. The structure of (international) cooperative networks is, however, not unique and has two clear precedents.

- In the case of negative lists of merchants internationally managed by VISA and Mastercard, it was already accepted by the art. 29 Working party that for the management of international cooperative networks the co-responsibility of financial institutions and data base operators (VISA, Mastercard) seems appropriate[17]. The database operators have no direct contact with the parties involved and in principle operate only in a "business to business" environment although their services are distributed in the retail circuit through their contracting parties.

[16] Cf. article 4.5.3 of the SWIFT general terms and conditions regarding the "Data Protection Obligations". In its contractual documentation SWIFT makes a distinction between the processing of personal data received from financial institutions through the signing or the use of the SWIFT services on the one hand, and on the other hand, the personal data contained in messages or files from financial institutions processed via the SWIFT services or products. With relation to the latter processing it is explicitly stated that the financial institutions are deemed to be the data controller.

[17] Cf. paragraph 16 of the Guidelines for Terminated Merchant Databases dd. 11th January 2005 which states that "The development and operation of a terminated merchant database require the joint action of two Participants acting as joint data controllers for any particular set of personal data relating to a specific merchant, namely 1) the Database Operator, and 2) the Participant that has a contractual relationship with the merchant."

- The pyramid structure of existing computer reservation systems or "CRS" in the airline sector appears to be a second precedent. In this case travel agencies and airline companies (amongst others) enter personal data in their reservation systems, the national distribution systems offer access to the reservation system under payment (reservation money) and finally the central management of the reservation system is looked after at the highest level. The Commission[18] and the French Data Protection Authority CNIL[19], in this case, already defended the point of collective responsibility.

Regarding the afore-mentioned cooperative networks, Data Protection Authorities hence appear In the last few years to take the point of view of co-responsibility of the professional users of the database and the controller of the database. .

Now that the context in which processing is performed has been pointed out, the question remains whether and to what extent SWIFT and/or the financial institutions determine the purpose and the means of the SWIFTNet FIN services. SWIFT is joint data controller in so far as it, together with others (the financial institutions), i.e. jointly, determines the purpose and the means of the processing.

- The SWIFT service is **not a mere transport service** and cannot be reduced to executor of a task on behalf of a third party, who would completely determine this task. In reality, it is the management of SWIFT rather than the financial institutions who determines the modalities for the supply of the services via the **accession contracts and technical standards which have in the main been fixed**. Moreover, if every individual financial institution would be able to ask for or implement a specific format or adjustment of data protection, it is obvious that the standardized functionality of SWIFT would be threatened. The preceding does not prevent that, in case a number of critical questions would be asked (SWIFT spoke of "market demand") regarding the adaptation of the service or the development of a new service, SWIFT adapts its services after close consultation with its members. A concrete example of this is the fact that the information processed by the SWIFTNet FIN service has already been adjusted upon the request of the Financial Action Task Force ("FATF") and after consultation with the financial institutions, in order to improve the methods of identification of natural persons[20].

  SWIFT is not a processor as it can take decisions regarding the purpose and the means of the processing, **decisions which moreover reach beyond the normal and legally defined "margins for manoeuvre" within which a normal processor can take decisions** when performing tasks entrusted to him. As SWIFT, with its processing in the framework of the SWIFTNet FIN service pursues its own goals, it is in the position to offer an added value with regard to the service provided by its competitors, amongst which its own customers. An illustration of the added value offered by SWIFT is the **automatic decryption of the data in the operations centres by which SWIFT performs a formal verification of the contents of each message**, in order to check the correct contents of the fields. Furthermore, only the management of SWIFT decides on the location of the operations centres and the distribution of the services through the location of its sales offices. Finally, SWIFT seems to have a wide autonomy regarding the implementation of its data protection policy on financial institutions in respect of **elements which fall outside the**

[18] Cf. the Commission's recommendation no. 01/98 regarding the "Computer Reservation System" dd. 14th December 1998.

[19] The Commission here refers to the example of computer reservation systems in the airline sector and which on the one hand contains clients such as the airline companies and travel agencies and on the other hand the managers of these reservation systems such as Galileo. The responsibility of both actors was already highlighted by the CNIL on 11th September 1996, on the occasion of the 18th international conference on the protection of privacy and personal data. Cf. the text on the site of the Canadian DPL: http://www.privcom.gc.ca/speech/archive/02_05_a_960918_03_f.asp

[20] According to the report

scope of the normal obligations of a processor or a processor agreement (cf. article 16 § 1 DPLDPL). For example, the "compliance policy ("no comment policy") differs from the policy of a number of (European) SWIFT clients and the privacy clauses which can be found in the various access contracts to the SWIFTNet FIN service. Fore-mentioned examples relate to the essential factual and legal aspects of processing which falls under the authority of the data controller and not under that of the processor.

- It is **not unusual for data controllers to have no direct contact with the relevant parties** and neither is this a requirement in the DPL when talking about the data controller. In other words: the application of the DPL is not excluded in a "business to business" context. Concrete examples of this type of controllers who do not have any direct contract or contractual relationship with the relevant parties have already been mentioned above (VISA, Mastercard, distribution companies and Computer Reservation Systems or "CRS").

- If, finally, one would pretend that only the 7,800 financial institutions bear the responsibility for the processing of personal data via the SWIFTNet FIN service, it would mean that the person seeking justice would be faced with such an enormous **scattering and judicial fractioning of the data controllers concerned** that it would make it in fact impossible to exercise any right provided under the DPL.

- SWIFT is finally not a processor as **it is not up to the processor, to take important crucial decisions at his own initiative and without any information to and agreement from the data controller during (almost) 5 years regarding the collection of data** by authorities such as the UST. It is clear that SWIFT took all the crucial decisions regarding the disclosure of data to the UST, and this without informing its 7,800 clients. This is shown by the following elements:

1. The deciding role SWIFT played in the disclosure of data to the UST appears from the continuous and secret negotiations with the UST and the agreements that were reached in this framework since the end of 2001. The concrete application of the subpoenas was secretly negotiated by SWIFT through the establishment of the "black box" construction, and later controlled by the implementation of search- and collection criteria, the audit process and the scrutinizers (cf. supra). SWIFT was also guaranteed that the source of the information would be kept confidential.

2. The crucial decisions were made in the Belgian head office and were followed through with regard to the disclosure of data to the UST. This concerned the decision to investigate the lawfulness of the American subpoena dd. October-November 2001 and to comply with it, the first decision to transfer information which was made following mutual consultations with the general advisor, the CEO, the head of audit and the delegation from the board of directors to the audit committee for the verification of the extraction process. The 7,800 clients of SWIFT were not informed about the secret decisions which were made by SWIFT in consultation with the UST.

3. The clients of SWIFT do not even appear to have been informed about the concrete scale and modalities of the transfer of data to the UST. This approach relies on the "no comment policy" in the compliance policy[21] which the management of SWIFT laid down in 1993.

[21] The declaration from SWIFT regarding compliance can be found on its website www.swift.com.

4. In the aftermath of the news articles from June 2006, SWIFT's clients did not even seem to be in a position to put a stop to the transmission of data to the UST. After the news articles regarding the subpoenas, an Austrian credit institution[22] requested SWIFT to put an end to the disclosure of data to the UST. In a letter dd. 9th August 2006, SWIFT refused to comply with its client request, stating that its US division is subjected to the jurisdiction of the US and that it must comply with the subpoenas on condition that they are valid and enforceable under American law.

On the basis of afore-mentioned considerations the Commission concludes that SWIFT is a data controller in the sense of the DPL with regard to the processing of data by its SWIFTNet FIN service. Hereafter, the Commission shall investigate whether there is any question of co-responsibility in so far as SWIFT determines the purpose and means for the processing of data in conjunction with the financial institutions.

D.2. Execution of international payment instructions by means of the SWIFTNet FIN service

Furthermore, the question arises whether the financial institutions assisted in determining the purpose and the means of the data processing which would make them co-controllers in the sense of the DPL.

Once again, it is important to picture the context in which the financial institutions transmit personal data to SWIFT. **In principle the financial institutions act at a different level, i.e. the level of settling payment instructions**. This type of data processing is different from the exchange of *financial messages* which are performed by SWIFT on a "business to business" (usually inter-bank) level. Of course, the exchange of financial messages hasa practical connection with payment instructions. The exchange and storage of data, *as a consequence of the payment instruction, seems to be required precisely to perform the transaction in a correct and safe manner within the inter-bank traffic*. The SWIFT processing does not take place "at the counter" in direct contact with the party who issues the payment instruction. On the contrary, it is done in the "back office" context of financial institutions where applications such as the scanning of payment instructions and inter-bank instructions are in principle performed in accordance with the professional standards and customs of every financial institution, the customs of the sector and the existing norms. The Commission concludes that the processing of "carrying out payment instructions" and "exchange of payment messages" are in practice often linked to one another, but that they are separate operations whose purposes and processing cannot be equated.

SWIFT states that the financial institutions are responsible for the execution of the processing which consists in settlement of international payments. Indeed, the financial institutions which use the SWIFTNet FIN service for this form of processing are not processors for SWIFT, and as such they do not act for SWIFT in any way.

[22] The Niederoesterreichische Landesbank – Hypothekenbank AG, Kremsergasse 20 in 3100 St.-Pölten, Austria

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 Commission 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, t**he financial institutions **often decide autonomously about the means used when settling payment instructions**. They have the freedom of choice to whether or not use the SWIFT service to send financial messages with regard to individual transactions. If necessary, they can use or develop alternative or rival services for the transmission of these financial messages within the inter-bank system (e-mail, fax, telephone, to a correspondent bank, …). 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 let them 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 VPN as a guarantee in order to safeguard the trust of their clients and their services to the maximum.

- The financial institutions **know the contractual framework of the SWIFTNet FIN service.** It comes out from the contractual documentation (Data Retrieval Policy[23]), and the SWIFT compliance policy shows that the clients of SWIFT **were aware of the general principle to transfer personal data subjected to subpoenas either served on them or on SWIFT**. SWIFT argued[24] 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.

- As professional service providers the financial institutions **must assess the possible implications and (privacy) risks for their clients relating to the SWIFTNet FIN service,** which they, as a professional service provider, underwrite. 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 in direct contact with the actual parties giving payment instructions, they actually play an **essential "counter role**". The Commission does not exclude that the financial institutions are considered to be a "middleman" in the exertion of the rights of the parties involved within the SWIFTNet FIN service framework, insofar as this takes place under a clear agreement with SWIFT as data controller in the frameworks of the SWIFTNet FIN service.

[23] Where 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."

[24] In reaction to a report of a Commission meeting dd. 22nd August 2006

Considering the afore-mentioned considerations the Commission is of the opinion that the financial institutions who are active in the international payment traffic on a "business to business" (inter-bank) level can likewise define the purpose and the means of the processing entrusted to them (the settlement of payment instructions from their clients). In so far as they make use of the SWIFTNet FIN service, they can – together with SWIFT - be deemed to be joint data controller with regard to the processing.

D.3. Responsibility of the National Bank of Belgium

In a joint draft resolution dd. 5th July 2006, the European parliament expressed the request to the member states[25] that they "make sure and ascertain that there is no legal void on a national level and that the community legislation on data protection also applies to the central banks" To this effect, the member states were asked to pass the results of this verification on to the European Commission, the Council and the European Parliament.

The Commission finds that the NBB as overseer neither determined the purpose nor the means for the processing of personal data via the SWIFTNet FIN service. Therefore, the NBB can not be a data controller in the sense of the DPL with regard to the afore-mentioned processing. The NBB, as overseer, was informed by SWIFT about the existence of the American subpoena in February 2002.

Considering the afore-mentioned draft resolution the Commission wanted to check with the NBB, as overseer, what "oversight" concretely entails, and to what extend the NBB, as overseer, considers it her task to watch that SWIFT would have sufficiently covered legal risks such as privacy risks. In its letter dd. 28th August 2006, the NBB responds
"(…) By virtue of article 8 of its Organic Law[26] the NBB watches over the proper functioning of the settlement and payment systems. This task fits in with the tasks of the European System of Central Banks (ESCB), especially article 22 of the ESCB statutes. This very specific task of the central banks is known as 'oversight'. This activity is performed from a system perspective, in which the proper functioning of the global payment- and settlement system is central in order to ensure financial stability and to avoid so called "system risks" with a domino-effect of bank's bankruptcies (…)"Furthermore, it was stated that
"The Bank (…) by virtue of its capacity of overseer does not bear any responsibility for the actions of SWIFT. SWIFT does not ask for nor receives approval or disapproval on decisions of management in operational, financial, legal or company law matters." and "(...) that in the course of 2002 the G-10 central banks consulted each other on the matter of the American subpoenas and that they came to the conclusion that these subpoenas fell outside the scope of the oversight of the central banks., no other new elements subsequently arose which would have induced the Senior Level Oversight Group to review that decision."

From the previous elements it comes out that the compliance with the DPL by SWIFT is not yet considered to be part of the individual or cooperative oversight.

However, to the extent that the NBB acts *as a client* of SWIFT and hereby entrusts personal data to the SWIFTNet FIN service, , the NBB can be considered as a controller as mentioned under section D.2..

[25] Joint draft resolution on the interception of bank transfer details from the SWIFT system by the American secret services.
[26] Act dd. 22nd February 1998 regarding the organic statute of the National Bank of Belgium

E. INVESTIGATION INTO POSSIBLE VIOLATIONS OF THE DPL

The request for an opinion concerns the question if SWIFT has possibly violated the DPL . The question whether the (Belgian) financial institutions violated the DPL, falls strictly speaking outside the scope of the opinion and cannot be investigated by the Commission in the limited time available. Considering that the Commission is however of the opinion that this is a case of co-controllership on behalf of the financial institutions, the Commission will remain further available to rule on any possible infringements by individual (Belgian) financial institutions.

The Commission stresses that there are fundamental differences between the EU and the US regarding the legislation and principles which regulate the processing of personal data. The processing of personal data under European law is characterized by a high level of protection which was introduced in Europe by virtue of the applicable treaties such as article 8 ECHR, the Treaty no. 108[27] and the applicable European Directives such as the 95/46/EG Directive.

The Commission highlights a few common mistakes that sometimes arise in relation to the notions "adequate protection" and "respect of the norm or the privacy law". The Commission stresses that, for the interpretation of these notions, it is not sufficient to provide control by external audit, to respect technical standards or norms (for instance ISO) or to provide adequate technical security measures. The applicable principles under the DPL reach way further.

Hereafter we will examine whether SWIFT complied with all applicable principles of the DPL, even if it would already have achieved a high level of protection. In the evaluation a distinction was made between the question whether on the one hand any infringements to the DPL were committed within the framework of the normal functioning of the SWIFTNet FIN service and whether on the other hand infringements on the DPL were committed within the scope of the transfer of data to the UST.

E.1. Did SWIFT infringe the DPL in the framework of the normal functioning of the SWIFTNet FIN service ?

E.1.1. legal basis (article 5 b) DPL and article 7 b) 95/46/EG Directive)

By virtue of article 5 of the DPL, personal data of instructing parties or beneficiaries may only be processed in a restrictive number of cases. The processing of personal data in the frame of the normal functioning of the SWIFTNet FIN service seems legitimate insofar as these are necessary for the execution of the agreement between SWIFT and the concerned credit institution (article 5b) DPL and article 7 b) 95/46/EG Directive)

[27] Convention dd. 28th January 1981 on the protection of individuals with regard to the automatic processing of personal data, B.S. (Belgian Law Gazette), 30th December 1993, enacted by the law dd. 17th June 1991 ratifying the Convention on the protection of individuals with regard to the automated processing of personal data, done in Strasbourg on 28th January 1981.

E.1.2. Obligation to provide information (article 9 DPL and article 11 95/46/EG Directive)

Insofar as SWIFT isconsidered to be a controller, it is also subjected to the obligation to provide information. This means that the natural persons whose data are exchanged in the payment messages must at least be informed in accordance with article 9 of the DPL. The data subjects should for example have known who the recipients of these data they transmitted to their credit institution might have been (SWIFT, authorities,…) and for which purposes these data could have been processed.

Considering that SWIFT collects these data on the basis of the instructions of financial institutions it does not directly receive the data from the persons concerned. In that case, according to article 9 § 2 of the DPL (article 11 95/46/EG Directive) "at the time of undertaking the recording of personal data, or, if a communication to a third party is envisaged, no later than the moment on which the data are first disclosed, the information must be provided, unless the data subject would already have been informed thereof" by the financial institutions. This means that, if SWIFT did not ensure that the financial institutions informed the data subjects in accordance with article 9 § 1 of the DPL and there is no specific saving clause on the obligation to provide information in the implementing order of the DPL, SWIFT did commit an infringement on article 9 § 2 DPL.

The fact that SWIFT does not have a direct relationship with the data subjects can finally not be considered as a valid reason for non-compliance with the obligation to provide information, for example through the financial institutions. Although the DPL does not concretely prescribe the manner in which the information must be provided, the context in which the data are processed can be taken into account, on condition that the chosen technique of giving information has the objective to inform the data subjects concerned clearly and effectively. The Commission already stated , in her opinion 48/2003of 18th December 2003, concerning the transfer of personal data to the United States by certain airline companies that "the manner in which the information is communicated to the client (is) moreover insufficiently clear, considering that this information is contained in the text regarding the general terms of transport and is only communicated upon request or over the Internet". In the context of mass manifestations such as football matches, the Commission[28] was of the opinion that the information could be provided on an individual basis (on the entrance tickets) or on a collective basis (e.g. through the installation of clearly visible billboards at the entrance of the stadium).

Considering its co-responsibility in view of the DPL, SWIFT insufficiently consulted the financial institutions in order to comply with the obligation to provide information (article 9 DPL). This resulted in the fact that insufficient information was provided to the data subjects and that article 9 of the DPL was not complied with.

[28] Advice 10/2005 dd. 15th June 2005.

E.1.3. mandatory reporting (article 17 of the DPL and article 21 of the 95/46/EG Directive)

Considering SWIFT is a data controller, it is in principle subjected to the obligation to notify which allows for a general, albeit minimal transparency and control. However, the Commission established that SWIFT did not submit any notification on the processing of personal data in the framework of the SWIFTNet FIN service, as opposed to any other form of processing such as its own personnel administration which falls outside the scope of this opinion.

Therefore, the Commission is of the opinion that **article 17 of the DPL was not complied with.**

E.1.4. Transfer of personal data to a country which has no appropriate level of protection (articles 21 and 22 and 39, 12° of the DPLL and articles 25 and 26 of the 95/46/EC Directive)

SWIFT should have taken into account the regulations regarding the transfer of data to third countries. The stipulations in the 95/46/EC Directive regulate this issue (chapter IV, in articles 25 and 26) and were partly adopted in the DPL, especially in articles 21 and 22 of the DPL.
SWIFT informed the Commission that it is of the opinion that the requirement of an appropriate level of protection under article 21 of the DPL would not be applicable to the processing in the frame of its SWIFTNet FIN service. A brief summary of their arguments:

- The ban on transfer of data (article 21 § 1) would not be applicable as the transfer was not made by the parent company out of Belgium.
- The ban on the transfer of data would not be applicable as the data were not transmitted to a third company and as, according to a company law rule, the SWIFT branch (operations centre in the US), is not a legal entity and would therefore, from a legal point of view always come under the parent company. This legal unity would have as a consequence that the processing of data in the frame of the SWIFTNet FIN service would remain subjected to an appropriate level of protection, i.e. Belgian law.
- Subsidiarily, insofar as the legal exceptions in article 22 § 1 DPL would be applicable, SWIFT argues that the transfer is necessary for the performance of a contract between the data subject and the data controller (article 22,2°), either because the transfer is necessary for the performance of a contract in the interest of the data subject (article 22, 3° DPL), either because the transfer is necessary or legally required on important public interest grounds (article 22, 4° DPL).
- The transfer occurs in a highly secured environment, with encryption of the contents of the messages.

Articles 21 and 22 of the DPL are applicable to personal data being transferred to a country which does not have an appropriate level of protection such as the US. Once again, the DPL uses a **functional criterion** in this regard. Considering that articles 21 and 22 of the DPL have been functionally described and constitute an imperative law of public order, company law rules can hardly overrule the entire protection policy of the 95/46/EC Directive.

The Commission considers that, in the framework of the normal functioning of the SWIFTNet FIN service, European messages are transmitted to the operations centres in Europe ànd the US. The fact that the data are transmitted to a branch is not a criterion for not applying the conditions of the law.

This transfer takes place on a daily basis and on a massive scale (11 million messages per day at the beginning of 2006). Upon transfer to the operations centres, the data are subjected to the entirety of the different types of processing[29] typical of the SWIFTNet FIN service.

The Commission notes that the fact of far-reaching security or the encryption of personal data does not prevent that the transfer of coded data still remains subjected to articles 21 and 22 of the DPL.

Furthermore, it is the opinion of the Commission that the exceptions provided for in article 22 of the DPL, do not apply to the processing via the SWIFTNet FIN service. Considering the alternatives from rival services which are available on the international payment market, the use of the SWIFTNet FIN service can hardly be considered necessary for every financial institution in order to carry out a payment instruction.

Finally, the notion "important public interest " must still be fulfilled under Belgian law, in compliance with the rules of law applicable in Belgium such as article 8 ECHR. SWIFT added that the mirror position of the operations centres is considered as a critical element in the global financial system. It states that the mirror position has been imposed by the overseers (G-10 central banks) for security and reliability reasons, as the SWIFT infrastructure is considered critical for the global financial industry. On a European level, it had already been ruled that the US does not offer an adequate level of protection according to the 95/46/EC Directive. Even if the global financial system would also affect public order in Belgium, it is still not a valid justification according to the 95/46/EC Directive for locating an operations centre in the US without an adequate level of protection.

As the US do not come under the category of countries which provide an adequate level of protection, the Safe Harbour Principles were specifically developed[30] for the US by decision of the European Commission. Moreover, in accordance with article 26, 2 of the 95/46/EC[31] Directive the Commission adopted a decision providing for appropriate contractual clauses to be used in the context of countries which do not guarantee an adequate level of protection such as the US. Finally there is the system of 'Binding Corporate Rules', i.e. the internally binding privacy code of conduct of a company, which can enable the transfer of data to third countries which do not have an adequate level of protection. **The Commission considers the system of binding corporate rules in accordance with article 26, 2 of the 95/46/EC Directive an appropriate and required measure to provide adequate guarantees for the daily and enormous transfers of data which are performed via the operations centres of a multinational company such as SWIFT**. This type of code of conduct must, in Belgium, however, be authorized by the King, upon advice of the Commission.

The Commission is of the opinion that the protection provided by SWIFT for the processing of data in its operations centres in the US does not comply with articles 21 and 22 of the DPL (articles 25 and 26 of the 95/46/EC Directive).

[29] In particular, the automatic decryption and formal verification of the data.

[30] See the Stipulation 2000/520/EG: of the Commission of 26 July 2000 in accordance with the 95/46/EG Directive of the European Parliament and the Council, regarding the appropriateness of the protection offered by the Principles of Safe Harbour with regard to the protection of privacy and the questions often asked in relation thereto, which have been published by the Department of Commerce of the United States (Notification thereof under number C(2000) 2441)

[31] See. http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

E.2. Did SWIFT infringe the DPL by transferring data to the UST?

Hereafter, the Commission wishes to investigate whether SWIFT infringed the DPL in the frame of personal data transfers to the UST.

E.2.1.. Legal basis (article 5 DPL and article 7 b) 95/46/EC Directive and article 8 ECHR)

The Commission emphasizes that it can not question either the legality, or the enforceability of the American legislation and of the American subpoenas, which clearly falls under the competence of the American authorities. However, the Commission can investigate whether a basis for legitimizing the execution of the American subpoenas can be found under the Belgian legislation on processing of personal data. By virtue of article 5 of the Data Protection Act, the personal data of the instructing parties or the beneficiaries can only be processed in a restrictive number of cases. SWIFT does not formally invoke a legal basis within Belgian law and only referred to the American subpoenas of which it states to have investigated the lawfullness and the enforceability. Prima facie, in particular articles 5 c) (legal obligation on behalf of the data controller) and 5 f) (protection of an important and legitimate interest of the data controller) seem relevant to justify the transfer of personal data to the UST.

As far as article 5 c) is concerned, the Commission endorses the view of the Group 29 dd. 1st February 2006 regarding the Sarbanes-Oxley legislation[32]. The Group 29 stated already that *"An obligation imposed by a foreign legal statute or regulation which would require the establishment of reporting systems 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 95/46/EC."*This means therefore that the American subpoenas cannot be considered as a ground for justification with regard to the processing of data in accordance with article 5 c) of the DPL.

Joining the point of view of the French Privacy Commission (CNIL) in the SOX-case[33], the Commission is of the opinion that it is impossible, in the case of the American subpoenas, to ignore the legitimate interest of SWIFT in the sense of article 5 f of the DPL. In other words, it cannot be denied that SWIFT has a legitimate interest in complying with a valid and enforceable subpoena under American law. When not complying with these subpoenas, SWIFT runs the risk of incurring civil sanctions under American law. Therefore, the Commission is of the opinion that the data transfer to the UST is **based on a legitimate and important interest on behalf of SWIFT in the sense of article 5 f) of the DPL.**

[32] Cf. 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.

[33] CNIL, Advisory document adopted by the Commission on 10th November 2005 for the introduction of measures on professional warning signs, conform to the law of 6th January 1978 and modified in August 2004, with regard to information technology, files and freedom.

SWIFT, on the other hand, should have realized that **the exceptions under American law could hardly justify a secret, systematic and large scale violation of the basic European principles of data protection, which went on for years**. This basic principle can be found in the second paragraph of article 8 ECHR[34]. The strict basic requirements have already been highlighted several times by the ECHR in particular with regard to the testing of secret surveillance operations against criteria such as the required foreseeability of the standard and the requirement for sufficient and effective control measures[35].

E.2.2. Principle of proportionality (article 4 § 1, 3° of the DPL) and storage term (article 4 § 1, 5° of the DPL)

The Commission is of the opinion that in casu there seems to be a "conflict of laws" situation between American and Belgian law, which forced SWIFT to make difficult choices once they received the American subpoenas. In view of the principle of proportionality it is however of the essence to check whether SWIFT has tried to find a **balance between both legal systems and whether it adequately examined and applied alternatives under Belgian or European law**. The fact that SWIFT is subjected to subpoenas and actively negotiated with the UST on the application of the subpoenas does not prevent that the processing of information must be performed in complance with the principles of Belgian and European law.

Considering the principle of necessity, the question is **which alternatives were open to SWIFT once it was established that it was subjected to valid and enforceable subpoenas**. A number of options seem to have been available, in particular:

- The challenging of the subpoenas under American law

  When questioned why the subpoenas were not challenged before the judges in the US, SWIFT replied that the first subpoenas were served shortly after the events of September 2001. The subpoenas would at present be founded on legal grounds under American law (codified in the so called "Patriot Act"[36]). SWIFT stated moreover that the risk existed that the American judge would have ruled that SWIFT was obliged to communicate all data without any restrictions.

- The application of official procedures and treaties on judicial cooperation

  The recommendations and procedures which exist for judicial cooperation on international and European level and which are aimed at the prevention of and the fight against the financing of terrorism by giving access to data from financial institutions appear not to have been followed.

---

[34] Which goes as follows: *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

[35] Cf. the cases Rotaru versus Romania (§ 55 and following), which refers to prior cases such as Malone versus UK dd. 2nd August 1984, Series A no. 82, p. 32, § 67, and *Amann* versus Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II, § 56):

[36] De USA PATRIOT Act (Public Law 107-56) or in full the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 is an American bill (H.R.3162) which was enacted in 2003 by a majority of the American Congress. This bill has as objective to give the American authorities more powers to gather information and to intervene in case of a possible terrorist attacks (source: http://nl.wikipedia.org)

Hereby can be referred to the public recommendations of the FATF ("GAFI")[37]. The FATF is an inter-governmental body that was created in 1989 and whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The recommendation n° 40 of the FATF contains the provision that "*Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.*" *In addition, one can refer to the cooperation in the context of the "Egmont Group"*[38]*. Via this informal group, an exchange of financial information is operated via the financial intelligence units or "FIUs" of 101 countries with a.o. Belgium and the US. This exchange is operated via the Egmont Secure Web or "ESW".*

The above-mentioned alternative organisms and systems could, in the light of Directive 95/46/EC, offer additional guarantees for the exchange of information regarding money laundering and financing of terrorism. Finally, it must be pointed out that, as a result of the terrorist attacks of September 11, two international agreements[39] between the EU and the US were negotiated which were signed on 25th June 2003 but are at present awaiting ratification from both sides. According to article 18 of the Vienna Convention on the Law of Treaties[40], 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.

The Commission notes that **SWIFT limited itself to complying with American law and the search for solutions via secret negotiations with the UST**. The Commission regrets that at no stage a choice was made to negotiate afore-mentioned alternatives and to contact the European authorities[41] competent for data protection in order to test the mass transfer of personal data to the UST against European law.

As far as the principle of proportionality is concerned, the Commission considers that the massive secret systematic transfer of personal data over many years can be considered as a violation of article 4 §1, 3° of the DPL.

Finally, control on the storage period of the data in the black box must be considered essential in light of the compliance with the principle of proportionality. With regard to the storage period of the data a distinction is made between the normal storage period customary in the framework of the normal functioning of the SWIFT operations centres and the storage period which applies to the data in the black box which have been made available to the UST[42]. It comes out from verifications of the agreements between SWIFT and the UST that this is a matter of an **indefinite storage period**, so far beyond the normal storage period in the frame of the SWIFTNet FIN service, which is contradictory to the principle of proportionality. Initially the possibility exists to store messages in the black box as long as they present a possible benefit to an investigation. Afterwards, a provision was made that SWIFT could recover all non-extracted messages from the black box, albeit under

[37] As published on http://www.fatf-gafi.org. See http://www.fatf-gafi.org/dataoecd/42/43/33628117.PDF concerning the 40 recommendations.
[38] See http://www.egmontgroup.org/about_egmont.pdf
[39] "Agreement on extradition between the EU and the US" and the "Agreement on mutual legal assistance between the EU and the US". Cf. the publications on 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
[40] Treaty of Vienna on the law of treaties, 23rd May 1969, B.S. 25th December 1993, which came into force on 1st October 1992. The United States have signed this agreement.
[41] Taking the analysis of the overseers into account who already declared themselves incompetent in the matter of subpoenas.
[42] The storage period which the UST would observe with respect to data which it retrieved after extraction from the black box are unknown.

obligation to store these data for as long as the possibility exists for subpoena of these data (cf. supra B.4.1)). The Commission finds that this possibility for change of location of data (from the black box to SWIFT) is of little influence on the conservation period, which in principle remains indefinite, in particular, as long as the possibility of a subpoena for these data exists. The Commission further notes that no concrete verifications could be made regarding the concrete conservation period of data in individual cases. It can therefore not be excluded that data on certain persons can be stored in the black box for years on end without any independent verification.

On the basis of the afore-mentioned considerations the Commission is of the opinion that the afore-mentioned practice of massive, secret and systematic transfer of data to the UST for many years with an indefinite storage time constitutes **a violation of the principles of proportionality and limited storage period as expressed in articles 4 § 1, 3° of the DPL (proportionality) and 4 § 1, 5° (storage time) of the DPL pursuant to articles 6.1. (c) and 6.1. (e) of the Directive 95/46/EC. In its capacity of data controller SWIFT should have realized that these principles are considered fundamental to the European legal system.**

E.2.3.. Principle of finality

The Commission emphasizes that it recognizes the importance and the legitimacy of the world-wide fight against terrorism. However, crucial to the evaluation in light of the DPL is whether the subpoenas, in view of their wording, could indeed only be used in the fight against terrorism and whether they did not for example contain an authorization for other purposes, which has been suggested by certain media[43] sources. This aspect depends on the definition and communication of the purpose of processing on the basis of the duty to provide information, which is explained hereafter.

However, it is outside the competence of the Commission to question the legitimacy of the American subpoenas.

E.2.4.. The duty to provide information by SWIFT (articles 4 § 1, 2°and 9 § 2 of the DPL and article 8 of the ECHR)

The Commission finds that any form of control on the purpose stands or falls with the required transparency and the exact definition of the purposes of the processing. The Commission notes in that respect that

- The exact purpose of the processing of data (fight against terrorism) was in principle imposed and defined in the subpoena, which were always treated with confidentiality and non-transparency;
- The objectives formulated in the SWIFT communications to the general public prior to 23rd June 2006 (and thus to the data subjects) remained very vague and did not mention any clear link with terrorism (mention of “illegal activities” and “illegal behaviour” in the public compliance policy of SWIFT);
- It was only repeatedly specified in the general press releases after 23rd June 2006 that SWIFT merely passed on the data for “specific investigations into terrorism” (in the explanation regarding the compliance dd. 23rd June 2006 and the updates of this explanation after this date)

The Commission finds furthermore that the SWIFT “no comment” policy regarding compliance seems to be at odds with the requirement for transparency ensuing from Directive 95/46/EC and the second paragraph of article 8 ECHR. This policy was largely inspired by the strict confidentiality obligations imposed on SWIFT in the framework of the individual investigations of the UST, the

[43] Cf. for example an article in Knack dd. 9th August 2006 in which the author suggests that there is rumour of cases which are not related to terrorism such as “a drug related case”.

general rules on confidentiality and duty for discretion which apply in the world of financial services and finally, the commercial interests and the risk to the SWIFT reputation.

The delicate question must however be asked **where a balance can be found between the high degree of confidentiality granted by SWIFT to the system, the width of the processing ensuing from the subpoenas, and on the other hand the various obligations with regard to transparency which SWIFT as a data controller** bears in accordance with articles 4 § 1, 2°of the DPL (required definition of finality in privacy policy) and 9 § 2 of the DPL (obligation to inform). On the other hand, the question arises to which extend SWIFT could and had to inform the financial institutions and the data subjects about the transfer of data via the UST.

The Commission is aware that legal or conventional confidentiality obligations do exist, both in the case of American subpoenas and Belgian subpoenas, which makes that the normal duty to provide information to the data subject (suspect, who is the subject of the subpoena), will not always be applicable when complying with a subpoena.

The Commission however, points to a fundamental difference between the UST subpoenas and the subpoenas under Belgian law. Under section B.2., it was already noted that the subpoenas from the UST must be qualified as **non-individualized mass requests ("Rasterfandung" "carpet-sweeping" technique)** operating on two levels, which is different from the Belgian subpoenas which are *ab initio* carried out on an individual case basis. It was noted under section B.2. in fine that the UST has "the full right under US law to subpoena SWIFT US branch to provide **all** SWIFT messages." This means that, for the year 2005 alone, a total number of 2,518,290,000 SWIFTNet Fin messages can be subject to the subpoenas[44]. SWIFT however states that she can only release these data upon application of an authorization procedure with the UST.

Considering the second paragraph of article 8 ECHR **the transparency obligations remain valid on a collective level**, thus in respect of the phenomenon of mass requests via European or American subpoenas.

Taking the secret, massive and unusual nature of the transfer of data into account, the Commission is of the opinion that SWIFT should at least have informed the financial institutions and the overseeing authorities (European authorities, DPL's amongst which the Commission) of the UST subpoenas.

E.2.5.. Obligation to notify

By virtue of article 17 § 6 DPL any transfer of personal data to a foreign country must be reported. SWIFT did notify many other types of processing[45] but did not notify the data transfer to the US and neither the "compliance" finality. This is remarkable as it is certainly not unusual for financial institutions and other financial service providers to notify their "compliance" finality and international transfers separately to the Commission. Indeed, references to "compliance" processing pursuant to the law of 11th January 2003[46] by the financial institutions are quite common.By not making any mention of the data transfer to the US and the compliance purpose within the framework of the subpoenas in its notification, **SWIFT violated article 17 § 1 of the DPL**.

[44] a Figure mentioned in the same letter of SWIFT of 14 September 2006. One can also start from the average and normal daily message traffic via SWIFTNet FIN which lies somewhere in between 6.9 million (2005) and 11 million messages per day (start of 2006) which, in its totality, can be subjected to subpoenas.
[45] In particular management of membership, clients,…
[46] Law on the prevention of the use of the financial system for the laundering of money and the financing of terrorism

E.2.6.. Requirement for independent control on data transfer (article 28 of Directive 95/46/EC and article 8 of the ECHR)

Prior to the news articles of June 2006, only the SWIFT management seemed to be acquainted with the modalities of the transfer to the UST[47]. The independent control required under article 28 of Directive 95/46/EC seems to have been largely hindered by the fact that the mass data transfers, on the part of SWIFT, was treated with the highest form of confidentiality. And thus neither the financial institutions concerned, nor the European authorities competent for data protection were informed of the mass phenomenon of the American subpoenas

The requirement for an independent control ensues however from the second paragraph of article 8 of the ECHR. In the Rotaru case the ECHR stated "The rule of law implies, among others, that an intrusion by the executive authorities on an individual's rights should be subject to effective supervision, which should normally be carried out by the judicial power, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (…)"[48]

By maintaining the mass and secret surveillance without the knowledge of the competent European data protection authorities, and without any independent control within the US (the only control carried out was by companies in the private sector, i.e. SWIFT and its auditor) **an infringement on the requirements under article 28 of Directive 95/46/EC was committed**.

E.2.7.. Prohibition on further transfers to recipients of data like the UST (articles 21 of the DPL and 25 and 26 of the 95/46/EC Directive)

In the absence of applicable saving clauses in the sense of article 22 of the DPL and 26 of Directive 95/46/EC (cf. supra), the Commission points to the fact that the transfer of data to the UST can not be effectively regularized by adopting "contractual clauses" or "binding corporate rules" within the SWIFT group.

Just like in the PNR-precedent it seems that in relation to these so-called onward transfers, specific agreements between the US and the EU are required in order to ensure that the recipient of the data (UST) will endorse in an appropriate way the rules of adequate protection under European law. The art. 29 Working Party has issued opinions in this context, concerning articles 25 and 26 of Directive 95/46/EC[49]. SWIFT might have used the existing GAFI agreements as a starting point, but the question is why this option was not taken.

Considering the fact that the recipient of the data (UST) was never subjected to an appropriate level of protection in accordance with article 21 of the DPL and Directive 95/46/EC, the Commission is of the opinion that SWIFT **violated article 21 § 1 of the DPL**. It can be considered a serious error of judgement on the part of SWIFT to subject a mass quantity of personal data in a secret and systematic manner for years to the surveillance of the UST without at the same time

[47] Apart from the fact that the NBB as "lead overseer" was notified of the existence of the first subpoena and that the financial institutions may be considered to be very familiar with the practice of subpoenas and the fact that the SWIFT transactions were considered to be subjected to these subpoenas according to contractual documents.

[48] "*The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55)."*

[49] Cf. the work document dd. 24th July 1998 of the Group 29 regarding the transfer of personal data to third countries: application of articles 25 and 26 of the EU directive on data protection, published at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1998_en.htm

informing the European authorities and the Commission in order to reach a solution under Belgian and European law.

FOR THESE REASONS

On the basis of her general investigation, the Commission is of the opinion that

- The DPL is applicable to the exchange of data via the SWIFTNet FIN service;

- SWIFT and the financial institutions bear joint responsibility in light of the DPL for the processing of personal data via the SWIFTNet FIN service;

- SWIFT is a data controller of the personal data which are processed via the SWIFTNet FIN service;

- The financial institutions are data controllers as they co-determine the objective and the means to perform payment instructions in the inter-bank traffic. The financial institutions in particular, at an inter-bank level, choose to process financial messages with regard to these payment messages via the SWIFTNet Fin service;

- As far as the normal processing of personal data in the framework of the SWIFTNet FIN service is concerned, SWIFT should have complied with its obligations under the DPL, amongst which, the duty to provide information, the notification of the processing and the obligation to provide an appropriate level of protection conform to articles 21 § 2 of the DPL;

As far as the communication of personal data to the UST is concerned, the Commission is of the opinion that SWIFT finds itself in a conflict situation between American and European law and that SWIFT at the least committed a number of errors of judgement when dealing with the American subpoenas. Iit must be considered a serious error of judgement on the part of SWIFT to subject a massive quantity of personal data to surveillance in a secret and systematic manner for years without effective grounds for justification and without independent control in accordance with Belgian and European law;

- In this context SWIFT should from the beginning have been aware that, apart from the application of American law, also the fundamental principles under European law must be complied with, such as the principle of proportionality, the limited storage period, the principle of transparency, the requirement for independent control and the requirement for an appropriate level of protection. These requirements are indeed formulated in the second paragraph of article 8 of the ECHR, Treaty no. 108, the Directive 95/46/EC and the DPL and are applicable to SWIFT. The Commission also refers to the international precedent in the PNR-case. The authorities competent in data protection (the Commission, its peers and the European Commission) should have been informed from the beginning, which would have made it possible to work out a solution at European level for the communication of personal data to the UST, with respect for the above-mentioned principles which apply under European law. For this purpose, the Belgian government could have been asked for an initiative at European level.

Considering the complexity of the issue and its importance, the Commission remains available to issue further guidance.

The administrator,	In the absence of the President, The Vice-President,
(sign.) Jo BARET	(sign.) Willem Debeuckelaere

NON-OFFICIAL AND TEMPORARY TRANSLATION as of 29092006

A. INTRODUCTION 2
B. FACTS AND LEGAL CONTEXT 3
B.1. SWIFT 3
B.1.1. Description of the data flow and data which are processed via the SWIFTNet FIN service……..3
B.2. Subpoenas……..5
B.3. Reaction from SWIFT to the subpoenas……6
B.3.1. Negotiations with UST……..6
B.3.2. Information to the Supervisors……7
C. APPLICABILITY OF THE DPL 8
C.1. Territorial scope……8
C.2. Substantive scope……8
D. OPINION ON WHETHER SWIFT, THE FINANCIAL INSTITUTIONS AND THE NATIONAL BANK OF BELGIUM ARE DATA CONTROLLERS OR PROCESSORS……9
D.1. The processing of data in the framework of the SWIFTNet FIN service……9
D.2. Execution of international payment instructions by means of the SWIFTNet FIN service……13
D.3. Responsibility of the National Bank of Belgium……..15

E. INVESTIGATION INTO POSSIBLE VIOLATIONS OF THE DPL 16

E.1. Did SWIFT infringe the DPL in the framework of the normal functioning of the SWIFTNet FIN service ? 16
E.1.1. legal basis (article 5 b) DPL and article 7 b) 95/46/EG Directive)……..16
E.1.2. Obligation to provide information (article 9 DPL and article 11 95/46/EG Directive)17
E.1.3. mandatory reporting (article 17 of the DPL and article 21 of the 95/46/EG Directive)……18
E.1.4. Transfer of personal data to a country which has no appropriate level of protection (articles 21 and 22 and 39, 12° of the DPL and articles 25 and 26 of the 95/46/EC Directive)……18

E.2. Did SWIFT infringe the DPL by transferring data to the UST?.....20
E.2.1.. Legal basis (article 5 DPL and article 7 b) 95/46/EC Directive and article 8 ECHR)……20
E.2.2. Principle of proportionality (article 4 § 1, 3° of the DPL) and storage term (article 4 § 1, 5° of the DPL……21
E.2.3.. Principle of finality……..23
E.2.4.. The duty to provide information by SWIFT (articles 4 § 1, 2°and 9 § 2 of the DPL and article 8 of the ECHR)……23
E.2.5.. Obligation to notify……25
E.2.6.. Requirement for independent control on data transfer (article 28 of Directive 95/46/EC and article 8 of the ECHR)……25
E.2.7.. Prohibition on further transfers to recipients of messages like the UST (articles 21 of the DPL and 25 and 26 of the 95/46/EC Directive)……26