Free Translation – Original in French
Translated by SWIFT scrl

Decision of 9 December 2008

Object: Control and recommendation procedure initiated with respect to the company SWIFT scrl

The Privacy Commission;

Having regard to the Act of 8 December 1992 *relating to the protection of privacy with respect to personal data processing* (hereinafter the "Privacy Act"), and in particular Article 30, §1;

Having regard to its Internal Rules (hereinafter, "IR"), and in particular Articles 37 to 39;

Having regard to the European Commission's request addressed to the Belgian Government to ensure that the SWIFT company respects the European legislation relating to the protection of personal data and to take all necessary measures in this regard;

Having regard to the control that it conducted and the information that it collected;

Having regard to the hearing of the company SWIFT, represented by Mr. T. VAN OVERSTRAETEN and Ms. S. ROUSSEAU, members of the Brussels Bar, and the briefs and written responses submitted by the latter;

Having regard to the adversarial procedure;

Having regard to the report prepared by Mr. S. VERSCHUERE, vice-president;

Issues on December 9, 2008, the following decisions:

I. THE PROCEDURE

I.1. SEQUENCE OF THE PROCEDURE

1. During its session of May 23, 2007, the Privacy Commission (hereinafter the "Commission") decided to initiate a recommendation procedure (Article 30, §1 of the Privacy Act) with respect to the company SWIFT. SWIFT was informed thereof orally on May 24 in the framework of a meeting with its representatives and the President of the Commission, and then by letter dated June 11, 2007. The Commission's Vice-president was appointed as rapporteur.

2. In the framework of the recommendation procedure, SWIFT has had the opportunity to develop and express its position pursuant to Article 30, §2 of the Privacy Act and Article 21 of the IR of the Commission. The following actions have been carried out:

- an inventory of exhibits was drawn up for the recommendation procedure by the Commission's secretariat and was communicated to SWIFT on August 1, 2007;
- SWIFT's attorney was heard by the President on August 16, 2007;
- by letter dated September 7, 2007, SWIFT communicated its first arguments to the Commission and sent the inventory of its file of exhibits;
- SWIFT was heard by the Commission during its session of September 19, 2007;
- further to the explanations provided by SWIFT during said hearing, the Commission submitted additional questions to SWIFT by letter dated October 23, 2007, together with the minutes of the hearing. SWIFT responded to the questions and formulated comments with respect to the minutes of said hearing by letter dated November 16, 2007;
- during its session of December 19, 2007, the Commission set the course of the procedure: drawing of provisional conclusions submitted to the adversarial review of SWIFT within a deadline of 30 days and, in case SWIFT would wish so, a new hearing to hear the arguments of the company;
- SWIFT expressed its wish to be heard again after having communicated its replies and comments on the provisional conclusions that were to be provided to it;
- by letter dated April 14, 2008 sent to SWIFT's attorney, the President and the rapporteur agreed, by preference and to the extent possible, to set a timetable for the remainder of the procedure in agreement with SWIFT after the latter would receive the provisional conclusions, taking into account the fact that the 30-day deadline could be reasonably extended if one element or other should justify it;
- provisional conclusions were drawn up under the responsibility of the rapporteur and communicated to SWIFT by e-mail and by registered mail dated April 23, 2008;

- on May 19, 2008, the President and the rapporteur held a meeting with SWIFT's representatives to examine a series of claims and remarks formulated by SWIFT based on the communicated conclusions: **(1)** SWIFT wished to access all documents examined or obtained from various sources by the Commission's secretariat and which had not been used at that stage, in order to ensure that they would not contain elements that the company would deem useful or necessary for the debate; **(2)** noticing that the provisional conclusions called upon facts that had not been exploited so far, SWIFT considered that certain facts, although described on the basis of documents in possession of the Commission or communicated by the Company, were established in a overly general way, even imprecise, and that their exploitation thus became ambiguous, problematic or even erroneous;
- on the basis of a proposal of the President and the rapporteur, the Commission decided, during its session of May 21, 2008, to grant access to all documents in its possession to the attorneys designated by SWIFT, and to communicate the exhibits for which a copy would be requested, without prejudice to confidential elements or documents that could in any event not be used; if a confidential document would turn out to contain an element favorable to the positions defended by SWIFT, the rapporteur and the attorneys of the company could agree to use its obvious meaning without citing the source thereof;
- the entire file of the Commission's secretariat was examined by SWIFT's attorneys on May 30 and June 6 and 11, 2008; a copy of the requested exhibits was provided; they constitute the second file of the Commission's exhibits;
- it has moreover been agreed that SWIFT could provide additional elements or information relating to the facts invoked in the provisional conclusions;
- during its session of June 11, 2008, the Commission set a timetable for the remainder of the procedure, taking into account these new developments: **(1)** the written responses to the final conclusions drafted under the responsibility of the rapporteur should be filed with the Commission's secretariat by September 17, 2008 at the latest (a French version will be sufficient for the procedure); **(2)** SWIFT will be heard during the session of September 24, 2008; **(3)** the Commission will render its decision on Wednesday October 8, 2008; this decision will be preceded by an adversarial debate regarding the publication of the decision if SWIFT should file a separate request in that respect; if such potential request were attached to the written responses to the conclusions, the debate will take place on September 24 after the debate on the merits of the matter; **(4)** the additional exchanges and intermediate actions must be carried out in such a way as to comply with this calendar;
- SWIFT was informed of this timetable by letter dated June 13, 2008;
- on June 25, the rapporteur together with the ff. director and a member of the secretariat went to SWIFT's head office; he received explanations from various officers of the company; additional documents were requested, which were then provided by SWIFT;

- the rapporteur considered that, in light of the quality and of the amount of information gathered, the latter should be rigorously examined and clarified to be integrated in a coherent reasoning from which useful conclusions could be derived; five additional meetings took place with SWIFT's representatives and the rapporteur; documents relating to the (factual and legal) context of the personal data transfer to the U.S. Treasury (UST) were sought out and gathered, to constitute the third file of exhibits of the Commission;
- in light of these developments, the Commission responded to a request of SWIFT and amended the timetable of the procedure during its session of 3 September: **(1)** the written responses to the conclusions shall be filed with the secretariat of the Commission by October 3, 2008 at the latest; **(2)** SWIFT shall be heard on October 8, 2008; **(3)** the Commission shall start its deliberations immediately after this last debate;
- the (definitive) conclusions were drafted on the basis of the substantiated file, under the rapporteur's responsibility, and have been submitted for SWIFT's adversarial comments; they were communicated to SWIFT by e-mail and postal registered letter on September 17, 2008;
- SWIFT communicated its written responses to the conclusions of the rapporteur on October 3, 2008 and was heard on October 8, 2008; SWIFT afterwards communicated additional information, documents and clarifications in writing on November 26, 2008 in order to respond to certain questions which had been formulated during the debate dated October 8 and to confirm the responses which had been provided;
- during its session of November 26, 2008, the Commission decided to close its deliberations and to issue its decision on December 9, 2008, SWIFT having the possibility to express its point of view as regards the publicity of the decision, in accordance with Article 14 of the IR.

I.2. THE MOTIVATIONS AND THE OBJECTIVES OF THE PROCEDURE

3. Having assessed the reactions of the various actors and participants to the Commission's opinions 37/2006 and 47/2006 and to Group 29's opinion 10/2006[1] ("WP 128"), including the concrete measures adopted by SWIFT, the Commission considered that it was necessary to formally initiate the present procedure of recommendation in the framework of the control that it conducted vis-à-vis the company SWIFT in accordance with Article 37 of the IR:

- considering that the data processing carried out by SWIFT should be examined on the basis of the provisions of the Privacy Act and taking into account the concrete measures adopted by SWIFT since the abovementioned opinions of the Commission and of Group 29 and, as the case may be, be framed or accompanied by recommendations in order to ensure full compliance with the law;
- considering the certainty that the European authorities would require the Belgian authorities to adopt all measures necessary in order for SWIFT to comply with the European rules relating to personal data protection (requirement among others confirmed by the letter sent by J. FAULL to the Belgian government on July 23, 2007);
- considering that it was necessary to follow up on the claims of SWIFT in relation to the aforementioned opinions; SWIFT has disputed the fact that a legal classification could be attributed to it, without being able to present its position before the authorities due to render a decision, whereas such qualification has direct legal consequences for SWIFT (in terms of obligations) or is likely to significantly affect SWIFT (including in terms of image and reputation, if reproaches should derive therefrom); as opposed to the opinion procedure, the recommendation procedure allows those to which it is applied to intervene in said procedure;
- considering, more generally, the necessity to decide on the questions raised by SWIFT in its claims, and the obvious need to clarify the concepts of data controller and processor in the meaning of the Privacy Act, especially in case of multiple, complex and interlocked operations carried out in the framework of permanent processing systems and of large volumes of personal data transfers between numerous actors and numerous States[2];

---

[1] Opinion available on the Group 29 website at the following address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf

[2] This issue was discussed in recent lawyers' newsletters, in the doctrine (see for instance TREACY, B., "Current data protection issues for financial institutions- Part I: the 'controller' v 'processor' dilemma. Privacy & Data protection", volume 7, issue 6, 3-6) and during a workshop of the International Chamber of Commerce dedicated to the "the distinction between data controller and processor pursuant to Directive 95/46/CE", including on the basis of the "SWIFT case" (the Commission has received a summary of the various opinions expressed during that workshop).

confirming the importance of a clarification, the Belgian National Bank has indicated to the Commission, in a letter dated September 11, 2007, that “an uncertainty factor as regards responsibilities” was not acceptable.

II. BACKGROUND

II.1. THE OPINIONS OF THE COMMISSION AND OF GROUP 29

4. In its opinions No. 37/2006 of September 27, 2006 and No. 47/2006 of December 20, 2006[3], the Commission has informed the Belgian government of its legal analysis and of its position regarding the obligations applicable to SWIFT and to financial institutions, particularly Belgian institutions, pursuant to the Privacy Act.

5. The Commission had then considered that, as regards personal data processing in the framework of the SWIFTNet Fin service, SWIFT had not complied with the obligations it was held to, based on the Privacy Act, in its status of data controller. At stake was the lack of compliance with: the notification obligation, the information obligation and the limitations of personal data transfers to countries not members of the European Union (Articles 17, 9, 21 and 22 of the Privacy Act). As regards the communication of personal data to the UST, the Commission had considered that SWIFT should have, as of the beginning, been aware of and should have taken into account the fact that, in addition to the application of U.S. law, the fundamental rules of European law on data protection had to be complied with, in particular the proportionality principle, the limitation of the retention of data for the period required by processing requirements, the transparency principle, the requirement of an independent control and the existence – prior to any transfer outside the European Union – of standards ensuring an adequate level of protection in the country of destination. The Commission had moreover considered that competent authorities[4] should have been immediately informed of the communication requests formulated by the UST. This immediate information would have made it possible to establish at a European level a solution compatible with the European law requirements on personal data protection, which SWIFT remained bound by. Group 29, which is composed of the national authorities of all States of the European Union, then expressed its position in an opinion of November 2006[5]. This position was similar to the position expressed in the Commission's opinions, at least as regards the status attributed to SWIFT and the assessment of the facts and the decisions made by the company. SWIFT was informed of these various opinions.

---

[3] These opinions are available on the website of the Commission at the address http://www.privacycommission.be.

[4] The Commission, its counterparts in the other Member States of the European Union, Group 29 that is composed of the national authorities of all States of the European Union, the European Data Protection Supervisor (EDPS) and the European Commission itself pursuant to the competences granted by Directive 46/95/CE.

[5] Opinion available on the Group 29 website at the following address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf

II.2. THE TRIGGERING FACTS, THEIR HISTORY AND THE CONSEQUENCES THEREOF

6. The facts at the basis of the aforementioned decisions of the Commission and of Group 29 are, more indirectly, also at the basis of this recommendation procedure. They have already been presented in the previous decisions. It appears, however, that facts that were then ill-known or whose review did not appear as obviously necessary, have not been presented, exploited or appreciated to their right value.

7. This observation calls for a new description of the facts and of contextual elements required to assess them, particularly in the framework of this procedure and the objectives that it pursues.

8. On June 23, 2006, the *New York Times* widely reported that the company under Belgian law SWIFT, which operated an operational center based in the United States, had supposedly collaborated with the CIA and the U.S. intelligence agencies, by transferring to them, for more than four years, copies of messages exchanges with financial institutions of the entire world, the latter entrusting the transport and the temporary archiving of said messages to the good care of SWIFT. Such transfer was described as the core element of a secret governmental program of a widespread surveillance of financial transactions, in the framework of the policy of defense of the U.S. security adopted by the U.S. government and which was criticized for the scope of the exception powers that it used, without regard for the liberties and fundamental rights of individuals. The information was widely disseminated and commented on by the Belgian and European press. One Belgian newspaper had the headline, among others: "Les intrusions de la CIA dans les données confidentielles", and later: "La CIA dicte sa loi en Belgique et en Europe"[6]. Another presented the facts: "*het doorspelen van gegevens van banktransacties aan de Amerikaanse inlichtingendienst CIA*" and titled, shortly thereafter and in relation to an apparent "SWIFT-gate": "CIA-SWIFT aanslag op privacy"[7].

9. It soon appeared that SWIFT had not communicated data to the CIA, but that it had transferred copies of certain categories of interbank messages, for certain periods of time, to the "Office of Foreign Assets Control" (OFAC), a division of the UST. These transfers were carried out further to legal and binding injunctions ("subpoenas") addressed by the UST to the SWIFT branch in charge of the exploitation of the U.S. operational center. These successive injunctions (64 at the time the information went public) were addressed to SWIFT in the framework of the investigations

---

[6] Respectively (free translation from French) "The CIA intrusions in the confidential data" and "The CIA imposes its law in Belgium and in Europe", Le Soir, 26 and 28 June 2006.

[7] Respectively (free translation from Dutch) "the transfer of bank transaction data to the U.S. intelligence service CIA", "SWIFT-gate" and "CIA-SWIFT assault on privacy", De Standaard, 27 and 29 June 2006.

conducted in the United States for the fight against terrorism financing, whose responsibility had been entrusted to the OFAC. In addition to the U.S. legal provisions that were invoked, the injunctions were expressly motivated by the performance of obligations imposed on the States by Resolutions 1333 and 1373 of the United Nations Security Council and by the limits imposed by the compliance with such resolutions.

10. On 15 October 1999, the United Nations Security Council acting pursuant to Chapter VII of the United Nations Charter[8] adopted Resolution 1267 dealing with the situation in Afghanistan and with the fight against terrorist movements acting from said State. On December 19, 2000, the Security Council acting on the same basis adopted is Resolution 1333, which confirmed and amplified the measures and operative provisions foreseen by Resolution 1267 and structured the UN policy in relation thereto. Resolution 1333 was then confirmed on multiple occasions and its operative provisions were further detailed or accompanied by additional powers, including through Resolutions 1363 (June 30, 2001), 1378 (November 14, 2001), 1390 (January 16, 2002), 1452 (December 20, 2002), 1526 (January 30, 2004) and 1805 (March 20, 2008)[9]. Through Resolutions 1267 and 1333, as well as those that followed, the Security Council decided, among others:

- that "*all States shall*" take measures to "*freeze without delay funds and other financial assets of Osama bin Laden and individuals and entities associated with him as designated by the Committee, including those in the Al-Qaida organization, (…) and to ensure that neither they nor any other funds or financial resources are made available, directly or indirectly for the benefit*" of the designated individuals and entities;
- to create, pursuant to Article 28 of its Rules of Procedure, a committee of the Security Council composed of all members of the Council and to ask, among others, this committee to: seek "*from all States the reports on the measures that they will have undertaken in order to implement [the present resolutions]*" and "*to ensure the effective application of the decisions*" of the Council; to examine such reports and to report to the Council by presenting the observations and *"recommendations for strengthening the effectiveness of these measures*" (Resolutions 1267 and 1333); but also to "*to promulgate expeditiously such guidelines and criteria as may be necessary to facilitate the implementation of such measures*" (Resolution 1390); and then, the mandate of the committee being reinforced and extended, to ensure *"in addition to the oversight of States' implementation of the measures referred to (…), a central role in assessing information for the Council's review regarding effective implementation of the measures, as well as in recommending improvements to the measures"* (Resolution 1526);

---

[8] **Chapter VII** [of the UN Charter] - Action with respect to threats to the peace, breaches of the peace, and acts of aggression:

Article 39. The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

(…)

Article 41. The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures.

[9] All these resolutions have been adopted unanimously by the Council.

- to create, in order to support the committee, "*an expert committee* (thereafter monitoring group) "*in charge of monitoring the implementation of the measures set forth (…) considering the links that exist between the purchases of weapons, the financing of terrorism, money-laundering, financial transactions and drug traffic" as well as a "a team supporting the implementation of sanctions*" composed of 15 members, specialists in the areas at stake.

11. On September 28, 2001, the Security Council, further acting pursuant to Chapter VII of the United Nations Charter, adopted Resolution 1373, relating among others to the fight against financing of acts of terrorism. Such resolution was confirmed and further detailed on several occasions, including by Resolutions 1438 (October 14, 2002), 1140 (October 24, 2002) and 1450 (December 13, 2002), and the aforementioned Resolutions 1526 and 1805[10]. In Resolution 1373, the Security Council decided among others that all States must:

- "*prevent and suppress the financing of terrorist acts*" and "*freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts*";
- "*afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings*" and "*find ways of intensifying and accelerating the exchange of operational information*";
- "*become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999*".

12. The Security Council also decided to create another Council committee, consisting again of all its members and in charge of missions similar to those of the committee of Resolutions 1267 and 1333. In the course of the successive resolutions, the cooperation between these two official subsidiary bodies was structured and amplified. The reports of both committees are subject to periodic debates within the Security Council. The committee of Resolution 1373 is from now on identified at the international level as the "committee against terrorism" (CAT).

13. Generally, the decisions adopted by the Security Council pursuant to Chapter VII of the Charter are binding on the Member States of the United Nations and are to be the subject of cooperation between them[11]. The Security Council has moreover systematically declared itself

---

[10] All of these resolutions were unanimously adopted by the Council, with the exception of Resolution 1450 (14 votes in favor, 1 vote against).

[11] Including pursuant to the following provisions of the Charter:

Article 24.1. In order to ensure prompt and effective action by the United Nations, its Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf. (…)

Article 25. The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.

(…)

"*determined to adopt all measures necessary to ensure the full implementation [of the present resolutions], in accordance with the responsibilities that it is bound to pursuant to the Charter*", which it has done in the course of the successive resolutions, binding Member States more and more tightly[12].

14. On 9 December 1999, the General Assembly of the United Nations adopted the International Convention for the Suppression of the Financing of Terrorism, quickly ratified by most of the States, including Belgium and the Member States of the European Union. Such international convention provides, among others, that:

- "*Each State Party shall take appropriate measures, in accordance with its domestic legal principles, for the identification, detection and freezing or seizure of any funds used or allocated for the purpose of committing the [terrorism] offences set forth in Article 2*" (Article 8.1);
- "*States Parties shall afford one another the greatest measure of assistance in connection with any investigation or procedure (…), including assistance in obtaining evidence in their possession necessary for the proceedings*" (Article 12.1);
- "*States Parties shall cooperate in the prevention of the offences set forth in Article 2 by taking all practicable measures, (…), including: (a) (…); (b) Measures requiring financial institutions and other professions involved in financial transactions to utilize the most efficient measures available (…)*" (Article 18.1);
- the States Parties shall further cooperate "*in the prevention of offences by considering measures for the supervision, of all money transmission agencies (…)*" (Article 18.2) and by conducting "*inquiries concerning the movement of funds relating to the commission of such offences*" (Article 18.3).

15. There is no doubt that the injunctions addressed to SWIFT by the UST found a basis in the elements of international legality (otherwise undisputed) stressed above. There is also no doubt that the information collected by the UST while consulting the transferred messages have been exploited in the framework of international police and judicial cooperation aimed at fighting against the financing of terrorism, imposed on the States by the Security Council resolutions and the Convention of 9 December 1999. It moreover appears in the information and reports sent to the monitoring

---

Article 48.1. The action required carrying out the decisions of the Security Council for the maintenance of international peace and security shall be taken by all the Members of the United Nations or by some of them, as the Security Council may determine. **2.** Such decisions shall be carried out by the Members of the United Nations directly and through their action in the appropriate international agencies of which they are members.

Article 49. The Members of the United Nations shall join in affording mutual assistance in carrying out the measures decided upon by the Security Council.

[12] See in this regard J.C. MARTIN, Les règles internationales relatives à la lutte contre le terrorisme, Travaux du CERIC, Bruylant, Bruxelles, 2006, in particular pp. 421ff: ""Pour le première fois de son histoire, [le Conseil de sécurité] définit une infraction internationale in abstracto sur le fondement du chapitre VII de la Charte, selon la logique classique du droit international" (free English translation: "For the first time in its history, [the Security Council] defines an international infringement *in abstracto* on the basis of Chapter VII of the Charter, according to the classical logic of international law"), and the corresponding note 409: "Les Etats se voient obligés d'incriminer l'infraction internationale dans leur ordre juridique interne et de mettre en oeuvre certaines obligations de lutte et de coopération internationale" (free English translation: "The States are obliged to incriminate the international infringement in their jurisdiction and to implement certain obligations of war and international cooperation").

groups and support teams created by the Security Council resolutions that the United States have mentioned without reservation the surveillance that was exercised on the SWIFT messages available on the U.S. territory and have considered this surveillance as part of the operational cooperative mechanisms set up and supervised by the United Nations. The committees of the Security Council have moreover assessed the States' reports, have summarized them and, in the framework of their mission, have derived recommendations or guidelines therefrom.

16. As a consequence, the President of the Committee created by Resolution 1267 provides, as is, to the President of the Security Council the third summary report of the monitoring group, dated December 4, 2002, requesting him to communicate this report to all members and to publish it as a Council official document[13]. Section 31 of the report, in the summary presentation and the list of useful elements, stresses that:

> "*The settlement of international transactions is usually handled through correspondent banking relationships or large-value message and payment systems, such as the SWIFT, Fedwire or CHIPS systems in the United States of America. Such international clearance centers are critical to processing international banking transactions and are rich with payment information. The United States has begun to apply new monitoring techniques to spot and verify suspicious transactions. The Group recommends the adoption of similar mechanisms by other countries*."

17. The justifications given by the UST for the injunctions addressed to SWIFT and the conditions under which the transfer and the consultation of messages copies have been carried out must moreover be briefly repeated:

- SWIFT stores copies of the messages exchanged between financial institutions in its archiving system only for a period of 124 days; the UST considered that such storage period was too short for the needs of the investigations, when an indication would make it possible to presume the presence of useful information in certain messages exchanged at a given time, without that such indication be sufficiently detailed to make it possible to precisely identify the possible suspicious transaction at that time; the UST has thus considered that the messages relating to the suspicious periods should be isolated, copied and protected from destruction in order to be usefully exploited on the basis of precise information that would be collected afterwards.
- After having been forced to comply with a first injunction (issued in emergency immediately after the attacks of September 11, 2001) regarding messages exclusively identified on the basis of a time period, and accompanied by an undertaking that the collected information would only be used for the fight against terrorism financing (to the exclusion of any other investigation even criminal or for tax purposes), SWIFT has contested the subsequent

---

[13] Doc. Sec. Conc. UN of 17 December 2002 – S/2002/1338 – available on the website of the Security Council (heading margin reference on the status of the document "Distribution: General").

injunctions, which presented the same characteristics, considering that they were disproportionate compared to the pursued objective (in light of the sole criterion of the time period, not precise enough and not sufficiently motivated; in light of the absence of guarantee that the restrictions on exploitation of the information would indeed be complied with; also in light of the frequency of the subsequent injunctions and thus of the amount of information at stake compared to the lack of formal supervision and control).

- Rather than submitting the issue to a court, the UST granted to SWIFT a series of supervisory measures of the transfers and of control measures of the exploitation of the messages at stake. These measures were presented in the previous opinions of the Commission and will be repeated below when their impact has to be assessed in the present procedure. SWIFT considered that the guarantees obtained no longer made it possible to dispute the legality of the injunctions before a court (for a possible lack of proportionality) and moreover considered that, further to legal consultations and analysis, such guarantees were greater than what a court could have granted.
- Generally, these guarantees covered: **(1)** a strict definition of terrorism using the relevant provisions of international law; **(2)** the presentation of initial indications, in support of the injunction, other than the sole time period invoked so far; **(3)** the consultation of the obtained messages based on precise indications (names) and legitimated suspicions (prior information from another source) and the limitation of the retrieval and the exploitation only to what was revealed by such indications and to the sole antiterrorist investigations; **(4)** the necessity for the revealed information to be confirmed by other sources in order to be exploited (generally by the financial institutions issuer or recipient of the message) including before a court or in an official act; **(5)** the organization of an independent audit, together with a system of **(6)** permanent control of the consultation of messages held by the UST and of the legitimacy of the indications invoked and of **(7)** blocking of the access to the messages in case of doubt or problem.

- **The UST representations and unilateral undertakings**

18. On July 20, 2007, some UST representations ("Representations"), including unilateral undertakings, as well as the response of the European Commission and the Council of the European Union, accompanied by a declaration of the French delegation, were published in the Official Journal of the European Union[14]. These mutual undertakings are aimed at formalizing and guaranteeing the conditions which the UST injunctions to SWIFT must now comply with, and the limits of their

[14] O.J., volume 50, C 166, p. 17 through 27. A publication followed in the Unites States on 23 October 2007 (Federal Register, Vol. 72, No. 204, p. 60054).

exploitation and of the storage of the data so collected by the U.S. administration. Except for details as regards the duration of storage of the transferred messages, the rules thereby adopted correspond to the guarantees previously granted to SWIFT. The Representations authorize and also foresee the review of these rules by an independent "eminent European person", in addition to the already foreseen audits and controls. This person of reference has been appointed and is supported by a team of assistants. He will be given a quite significant and detailed mandate (as regards the scope of the audit he is to perform and the powers that have been attributed to him).

III. SWIFT'S POSITION AND ARGUMENTS

III. 1. DURING THE HEARING OF SEPTEMBER 17, 2007

19. In the framework of the recommendation procedure, the company SWIFT had the opportunity to present a first time its position before the Commission. The following paragraphs summarize the case developed by SWIFT with respect to three issues:

- compliance with the rules governing cross border flows of data (III.1.)
- compliance with the information obligation (III.2.)
- compliance with the notification obligation (III.3.)

20. SWIFT considers that it acts as a processor (in the meaning of Article 16 of the Privacy Act) for its clients, i.e. financial institutions, and this both for the personal data of the latter's clients contained in the messages transmitted through the SWIFTNet FIN service and for the personal data transmitted in response to the UST injunctions.

III.1.1. As regards compliance with the rules governing cross-border-flows of data (Articles 21 and 22 of the Privacy Act)

21. SWIFT indicates that, as a consequence of its adherence to the Safe Harbor program on July 19, 2007, there cannot remain any doubt that the data transfer that it has been entrusted with in the framework of the SWIFTNet Fin services is absolutely legitimate, as its undertaking to abide by the Safe Harbor principles makes it possible to ensure an adequate level of protection of these data in the framework of their transfer to the United States, pursuant to the Decision of the European Commission 2000/520/CE of July 26, 2000. Therefore, according to SWIFT, no recommendation is necessary in that respect.

III.1.2. As regards compliance with the information obligation (Article 9 of the Privacy Act)

22. SWIFT indicates that, according to Article 9 of the Privacy Act, the obligation to inform data subject lies with the data controller. In its capacity of processor acting on behalf of its clients (the financial institutions) in the framework of the SWIFTNet FIN service, SWIFT would thus not be legally bound by such an obligation.

23. SWIFT indicates that, without prejudice to such postulate, it has put in place two information channels: the first one is aimed at informing its clients (the financial institutions) through its policies (among others), and the second is aimed at informing the public in general through its website.

24. SWIFT concludes from the above that the detailed information that it provides to its clients (the financial institutions) allows them to adequately inform their own clients. The policies and the online Questions/Answers (see point II.1.2. and below) specify among others in that respect that the financial institutions must provide information to their own clients in relation to the processing of their personal data.

25. *Information on SWIFT's website* – On its website, SWIFT has made accessible to the public the various policies mentioned above as well as to the additional explanations on the UST injunctions to the extent that such information is public. A list of the most frequently asked Questions/Answers (location of the operational centers, reason for the mirroring of the processing and the data, implemented security measures) has also been published on its website.

26. SWIFT adds that it would be *impossible in practice* to directly inform the subjects whose data are contained in the messages that it transfers on behalf of its clients, for the following reasons:

- SWIFT is not in a position to directly inform the data subjects of the processing of their data as it has no contact with the latter, as opposed to its own clients (financial institutions);

- direct information of the data subjects would require that SWIFT open all messages sent by its clients to verify whether the messages relate or not to individuals and extract these subjects' contact details in order to contact them. SWIFT currently does not own the tool required to automatically extract the data of the persons whose personal data would be processed in the messages sent by its clients. The implementation of such a search tool would involve significant development costs and would require SWIFT to process more personal data than is necessary to provide its messaging service, which would be contrary to the Privacy Act and in contradiction to the interests of the data subjects. Such a procedure would, in its view, be largely disproportionate to the pursued purpose.

- direct information of the data subjects would be largely redundant as the financial institution clients of SWIFT already possess the tools to ensure the communication of the required information to their own clients, as they are in direct contact with the latter.

27. SWIFT also indicates that detailed information regarding the communication of data and their processing by the UST is set forth in a letter sent to the European Commission and to the Council of the European Union, published in the *Official Journal* of the European Union. For the sake of transparency, SWIFT has inserted a hyperlink to these documents on its website (see hereinafter).

28. SWIFT concludes that, in light of the above, it has adopted all measures in its power in order to ensure the complete information of all stakeholders, both as regards its SWIFTNet FIN service and the data transfer to the UST. Therefore, no recommendation in that respect is necessary.

III.1.3. As regards compliance with the notification obligation – SWIFT's status (Article 17 of the Privacy Act)

29. SWIFT admits that it has not notified the data processing *carried out in the framework of its SWIFTNet FIN service* as, in its view, it operates as a processor on behalf of its clients in the framework of such service. It would thus not be required to file a notification pursuant to Article 17 of the Privacy Act as, according to such provision, it is only the data controller that should notify the processing that it carries out to the Privacy Commission.

30. SWIFT adds that it is not required to notify the data transmission to the UST. It was legally compelled to provide these data to the UST, which required them in order to process them in the framework of the fight against terrorism. Since SWIFT was not involved in the determination of such purpose, or in the means implemented in the framework of such processing, it is not required to notify the same either. SWIFT adds in that respect that, not being a financial institution, it is not subject to the Law of 11 January 1993 *relating to the prevention of the use of the financial system*

for money laundering and terrorism financing purposes. As a consequence, it was not required to notify such processing for compliance purposes either.

31. SWIFT founds its reasoning, according to which it is not a data controller neither in the framework of the SWIFTNet FIN service, nor in the framework of the data transmission to the UST, on the following arguments:

- SWIFT does not define the purposes of the processing:
  In the framework of the SWIFTNet FIN service, these purposes – that is, according to SWIFT's terms, the communication of payment instructions or other financial operations in a form ensuring their legibility by the relevant actors, whatever their geographic location – are determined by its clients, i.e. the financial institutions.
  SWIFT recalls in that respect that it only has a limited access to the content of the messages that it transports. It only verifies, on an automated basis, their conformity with the applicable standards, in order to ensure a legible communication between the relevant financial institutions.

  In the framework of the data communication to the UST, SWIFT argues that it is the UST, and not SWIFT itself, that determines the purposes of the data communication and processing, namely the identification of elements making it possible to combat terrorism.

- SWIFT does not define the means of the processing:
  In the framework of the SWIFTNet FIN service, SWIFT immediately indicates that the setting up and development of its service (for instance the devising of the standards used to convey the information necessary to the accomplishment of the financial transactions, the principle of mirroring of the operational centers for security purposes) have been thought out by the financial institutions themselves or upon their request, in order to make it possible for them to carry out the communication necessary to the accomplishment of a financial transaction. SWIFT then adds that making certain decisions regarding the implementation and the architecture of said services does not deprive it of the status of processor. SWIFT invokes in that respect Article 16 of the Privacy Act, which does not exclude that a processor makes choices regarding the necessary modalities – such as security measures – to carry out the processing in accordance with the law. Similarly, the determination of certain means in the framework of the transport of data provided by its clients would not transform SWIFT into a data controller, in light of the absence of determination of the purposes on its part.

  In the framework of the communication of data to the UST, SWIFT underlines that the UST determines on its own the means that it wishes to use to process the data that SWIFT is bound to communicate to the UST.

32. On the contrary, SWIFT defends the theory according to which it acts as a processor on behalf of the financial institutions (clients).

33. In that respect, it relies on the contractual documentation relating to the SWIFTNet FIN service and on its various "policies", documentation according to which both its mission as processor and the fact that it is only authorized to act upon instruction of the data controller are described and recognized (Article 4.5.3. of SWIFT's general terms and conditions, sections 3.1 and 3.2 of the Personal Data Protection Policy).

In fact, SWIFT's role in the framework of the SWIFTNet FIN service is to transport messages on behalf of its clients. The measures adopted by SWIFT are aimed at ensuring the security of the processing that it is entrusted with, which is the first role of a processor pursuant to Article 16 of the Privacy Act. SWIFT also adds that both the representatives of the banks that participated in the

working group within which the aforementioned "policies" were revised and the Belgian federation of the financial sector (FEBELFIN) on behalf of Belgian banks confirm that SWIFT is a processor.

34. Similarly, the fact that SWIFT has obtained guarantees from the UST would in no way demonstrate that is has overstepped its role as processor. Thereby, SWIFT considers that it has complied with its obligation to ensure that the data that it is entrusted with are processed in optimal security conditions.

35. Finally, SWIFT indicates that the SWIFTNet Fin service is a mere transport service that does not per se require any processing of personal data.

36. SWIFT could, however, not consider deleting the fields mentioning the identity of the payers or of the payment beneficiaries as such fields derive from an obligation imposed by the FATF (Financial Action Task Force), confirmed by *Regulation (EC) No 1781/2006 of the European Parliament and of the Council of November 15, 2006 on information on the payer accompanying transfers of funds*.

37. SWIFT moreover stresses that national authorities for personal data protection do not agree on the status of SWIFT. It refers in that respect to an opinion of the Spanish Agency for data protection[15], which - according to SWIFT - concludes that SWIFT is a processor acting on behalf of its clients in the framework of the SWIFTNet FIN service. SWIFT also refers to opinions of the data protection authority of Schleswig-Holstein in Germany and of the Austrian Commission for data protection[16], according to which SWIFT would have been recognized as a "processor". SWIFT also relies on a letter predating the adoption of Direction 95/46/EC (18 July 1994) according to which, in response to the concern expressed by the European Banking Federation with respect to such issue, Mr. R. Vanni d'Archirafi (Directorate-General XV) has indicated that the role of intermediary bank during a transfer required by the execution of a payment order could be that of "*processing agents acting in the framework of a contract whose object is determined and bound by security obligations*".

38. SWIFT also sheds light on the risks linked to the data controller status. As data controller, SWIFT could be compelled to develop a search tool making it possible to identify, in all messages that it is entrusted with, the identity of the data subjects in order to comply with its obligations in terms of verification of the quality and proportionality of the data, the information of the data subjects and the setting up of their right of access. Thereby, SWIFT would process more data than what is necessary to carry out its messaging service, in contradiction with the spirit of the Privacy Act.

39. Finally, SWIFT foresees certain practical issues with its clients if it were to be qualified as data controller:

- as it does not have access to the personal data contained in the messages that it transports, SWIFT would not be able to ensure the compliance of its obligations as data controller: SWIFT could not verify that these data are adequate, relevant and non-excessive with respect to the purpose of the processing (Article 5 of the Privacy Act); SWIFT could not individually inform the data subjects (Article 9 of the Privacy Act) and would be unable to respond to an access request that it would receive (Article 10 of the Privacy Act);
- the notification standard form made available by the Commission on its website requires that, in case of multiple data controllers for the same processing, as it is the case in the

---

[15] Agencia espanola de proteccion de datos, Resolucion de archivo de actuaciones, Expediente n° E/00797/2006, 27 julio 2007.

[16] Datenschutzkommission, ref.: K121.245/0009-DSK/2007, 21 March 2007, Ruling of the Data Protection Commission to SWIFT SCRL.

framework of the SWIFTNet FIN service, the notification be jointly filed by all data controllers.

40. In light of these difficulties, SWIFT requests, in subsidiary order, that the Commission describes in a reasonable, precise and practical way **(1)** the legal obligations of a data controller which SWIFT should comply with considering the abovementioned limitations and the fact that these obligations may be borne by the financial institutions and **(2)** the outline of the notification that it would recommend.

III. 2. DURING THE HEARING OF OCTOBER 8, 2008

41. At the hearing of October 8, 2008, it was recalled that since SWIFT's first hearing, many meetings had taken place, including with the rapporteur, documents which had not been accessible until then could be consulted, an in-depth analysis had been carried out, which is based on a better knowledge, understanding and assessment of the facts.

42. SWIFT has acknowledged these results. According to the company, the rapporteur's Conclusions forms an inseparable part of the whole legal consequences that are mentioned therein, including as regards the responsibilities and the obligations of the various stakeholders at individual and collective levels. If the Commission were to decide not to follow the rapporteur's Conclusions in part or as a whole, SWIFT indicated that it wished to be informed in order to examine and to discuss with the Commission on the basis of the position developed in its reasoning of September 7, 2007 and this, before the Commission's decision becomes definitive and *a fortiori* public.

III.2.1. Analysis of the rapporteur's Conclusions

(A) Objective of the procedure and acknowledgement of SWIFT's initiatives

43. In the framework of the present procedure of recommendation, since its first reasoning of September 7, 2007, SWIFT stressed that it had taken all measures within its power in order to comply with the obligations that the Commission imposed on the company, while maintaining that it was not legally bound to comply with these obligations given its status of processor. These measures are mentioned in the rapporteur's Conclusions.

44. Given these elements, SWIFT noted that the rapporteur only retained the filing of the declaration of processing of personal data with the Commission as the sole requirement which had still to be carried out in order to comply entirely with the Privacy Act (points 29 and 210 of the rapporteur's Conclusions). The rapporteur clarifies the specific circumstances in which he considers that such declarations are necessary.

45. As a result, SWIFT indicated that it was of the opinion that it was not relevant to once again develop a reasoning in response to the Commission's previous allegations as regards the compliance with the information obligation and with the provisions regarding transfer for which, if still necessary, SWIFT refers to its reasoning developed on September 7, 2007.

(B) Description of the processing of personal data in the framework of the services provided by SWIFT

46. SWIFT noted that five categories of processing had been identified by the rapporteur:
- processing carried out by the banks for their own account;
- processing carried out by SWIFT on behalf of the community of users of its services;
- processing carried out by SWIFT on behalf of a specific user upon an individual's request (security copy for the bank in case of disaster);

- processing carried out by SWIFT in order to produce information on financial transactions;
- processing carried out by SWIFT in order to respond to binding injunctions legally addressed by a competent authority (debate regarding the U.S. subpoenas).

47. With respect to processing in response to injunctions from authorities, SWIFT acknowledged the rapporteur's Conclusions according to which the Privacy Act is not applicable to it, while disputing the fact that the company could be considered as being controller as regards such processing.

(C) The purpose of the processing

48. SWIFT noted that, further to a long analysis, the rapporteur has come to the conclusion that:

- the processing of the first three categories contribute to the security of the financial transactions by the automatic and secured transmission of standardized, integrated and directly exploitable information;
- the processing of the fourth category refers to the production of general information on the financial transactions;
- the purpose of the processing relating to the fifth category is the execution of the legal obligation (U.S. obligation, in this case) to which the controller is subject.

SWIFT indicated that it does not share the entirety of the rapporteur's legal analysis on this last point.

(D) The status of the parties at stake and the responsibility of the processing

SWIFT summarized in the following manner its understanding of the status of the parties at stake and the responsibility of the processing retained by the rapporteur:

- **The financial institutions**

49. When it acts in its status of the payer's bank, the beneficiary's bank or the bank which requires a copy of a message, the financial institution intervenes as controller. Since this question is not concerned by this recommendation, it will not be examined in further detail here.

- **The financial community of SWIFT client users**

50. The rapporteur analyzed in depth the decision-making process in place within SWIFT and its community of users in order to define who determines the means and the purposes of the processing with a view to identifying the body acting as data controller for each processing at stake.

51. The rapporteur identified a solution-sharing aimed at satisfying the community needs, of which SWIFT is the ultimate expression. His analysis allows noticing a real "community of interests", tacitly and informally constituted and whose collective rules of functioning are established, implemented and respected for more than thirty years.

52. The rapporteur therefore concluded that SWIFT expresses and materializes the decisions of this community and acts while being invested with a real *de facto* delegation by default. According to the rapporteur, the community processing applied to all messages for which the financial community of SWIFT client users is data controller are the following:

- decryption and reading of the messages for authentification purposes;
- validation (presence of mandatory content and legibility of the message) and certification of their integrity;

- re-encryption and new decryption for the purposes of a last encryption by way of a key which is provided to the bank;
- duplication and transfer to a data processing center in the United States of America and processing in mirror of the whole process (resilience);
- archiving for 124 days in both data centers;
- destruction of the archived copies after 124 days.

53. SWIFT indicated that this analysis is confirmed, among others, in the introduction of its 2007 annual report which is titled “Community inspired” and provides “We act as the catalyst that brings the financial community together to work collaboratively to share the market practice, define standards and consider solutions to issues of mutual concern and interest”. This introduction reflects SWIFT’S corporate purpose.

- **SWIFT on an individual basis**

54. SWIFT also added that further to its analysis, the rapporteur concludes that the only processing for which SWIFT possesses real power of assessment is what the company realizes on the data temporally archived, for purposes not directly linked to the execution of financial transactions or for their maintenance. In this regard, the rapporteur made the following distinction:

55. **(1)** Extraction of data and anonymization with a view to producing information on financial transactions: the requirements of processing of the data in this framework are set in consultation with the users in the Data Retrieval Policy, which indicates that SWIFT processes in this framework only anonymized data. With respect to such occasional processing, SWIFT mentioned that it does not dispute the status of controller.

56. **(2)** Communication of data in response to a binding injunction: SWIFT stressed that, on this point, the rapporteur’s Conclusions and the company’s position are different. SWIFT in fact rejects the status of controller as regards these processing. It indicated that, although these are envisaged and framed by the Data Retrieval Policy, SWIFT does not determine the purposes or the means.

57. While maintaining its point of view according to which the status of controller in this framework is not correct, SWIFT noted the limited consequences of such status as they result from the rapporteur’s Conclusions. It concluded, without any detrimental recognition, that there was an absence of pertinence of such status since the rapporteur admits that the data are transferred to the United States of America and as regards the further processing necessary because of the injunctions from the UST, the Privacy Act is not applicable (together with all consequences that such observation implicates, including the fact that no declaration is required).

(E) The obligations of the various stakeholders

58. SWIFT recalled that after having attributed the responsibility of each processing, the rapporteur has tried to describe in a pragmatic manner the obligations to be complied with for each of the stakeholder in the framework of the various forms of processing identified.

- **The obligations of the financial institutions**

59. Since the recommendation is not addressed to the financial institutions, their obligations are not examined in detail. Each bank is subject to the national law which is applicable to it.

- **The obligations of SWIFT community of users**

60. According to the rapporteur, SWIFT must be considered as a *de facto* delegate of the financial community of its client users. SWIFT indicated that the rapporteur mentioned expressly

that the envisaged delegation is a delegation by default. SWIFT must therefore only execute the obligations to which the financial community is subject so long as the members of this community are not in a position to comply with them.

61. SWIFT mentioned that since its reasoning of September 7, 2007, it indicated that it was not able to comply with an obligation which necessitates direct contact with the concerned persons (and, among others, a response to a request for access from a data subject) because it does not have the means to retrieve data allowing one to identify a data subject in the messages that it processes. If SWIFT were to comply with the obligations of the financial community on this point, it would have to develop an instrument allowing it to localize and manage the corresponding data, i.e. develop a system more intrusive in terms of protection of privacy and personal data than the current system. SWIFT mentioned also that such a system would certainly be rejected by the banks. Besides, while banks already comply with these obligations on an individual level, why should these obligations be doubled by imposing them on their delegate?

62. The rapporteur recapitulated the various obligations of the financial community of SWIFT's client users, including the transfer of data outside the European Union, to come to the conclusion that the only obligation which, in practice, is not complied with by the financial institutions of this community would be the declaration of processing for which this community is controller. The rapporteur therefore suggested that SWIFT file this declaration on behalf of this community. SWIFT prepared a draft declaration in this regard and indicated that it was ready to comply with this requirement on behalf of the financial community so long as the Commission confirms that this declaration obligation is the only one still to comply with by SWIFT in this regard.

- **The obligations of SWIFT**

63. **(1)** Extraction of data and anonymization in order to produce information on financial transactions: SWIFT indicated that the rapporteur considers these operations to comply with the conditions for the further processing as set out by the King in accordance with the law. The rapporteur adds also that the right of access, rectification and opposition is not conceivable regarding the anonymized data. Besides the declaration obligation, SWIFT therefore concluded that, according to the rapporteur, the other possible obligations of the Privacy Act are, either already complied with, not applicable or benefit from legal exceptions. This is, among others, the case of the individualized information obligation which, in any event, is not conceivable for SWIFT to the extent that such individualization would be far too disproportionate as regards the objective of protection. SWIFT also recalled that it published general information in this regard on its website for transparency purposes.

64. **(2)** Communication of data in response to a binding injunction: SWIFT stressed that the rapporteur came to the conclusion that communication of data to the UST is no longer subject to the obligations of the Privacy Act because of the mere quality of such transfer. SWIFT does therefore not have to comply with any obligation of the Privacy Act in this regard and no declaration must therefore be filed with the Commission in this regard.

(F) Analysis regarding the communication of data to the UST

65. SWIFT indicated that these communications of data have been carried out in accordance with binding and legal injunctions. In doing that, SWIFT responded to a U.S. obligation as well as to an international obligation (resolutions of the United Nations). SWIFT recalled the protections and guarantees obtained from the UST which have been confirmed in the "Representations" towards the European Union.

66. SWIFT indicated that it does not share one of the legal arguments developed by the rapporteur when he considers that the principles of the Safe Harbor do not guarantee by their own

means a transfer ensuring an adequate level of protection of data and that it is necessary to complete them with other guarantees, in this case the UST Representations.

67. According to SWIFT, what if other authorities required an access to these data exercising legally the binding powers with which they are invested? The answer to this question requires a political solution, which exceeds SWIFT's powers and are not either within the Commission's powers.

68. SWIFT also repeated its wish not to dispute past events. However, it considers that it is important to recall that the company tried to comply with the law when it received injunctions further to the attacks of September 11, 2001. The installation of the operational center in the United States of America took place *in tempore non suspecto*. SWIFT would therefore appreciate it if the suspicions of infringement of which it was the object were clarified.

III.2.2. SWIFT's position and conclusion

69. In conclusion, SWIFT could not agree with the rapporteur's reasoning on two points: **(1)** the status of controller in case of subpoena and **(2)** the necessary combination of the Safe Harbor principles and the "Representations" to satisfy the requirement of a transfer ensuring an adequate level of protection to the United States of America.

70. If SWIFT does not necessarily share all elements of the legal analysis carried out by the rapporteur, it recognizes, however, the importance of the work accomplished.

71. Given the progress made, and hoping that the consequences described in the rapporteur's Conclusions as regards SWIFT's obligations will be confirmed in their entirety by the Commission, the company launched the following five initiatives:

- preparation with the assistance of the rapporteur and its team of a declaration as a *de facto* delegate by default of the financial community of SWIFT's users;
- preparation with the assistance of the rapporteur and its team of a second declaration as controller as regards the extraction and anonymization of data in view of producing information on financial transactions;
- reflection on the re-examination of SWIFT's policies to determine to which extent these should be modified to take into account the Commission's decision;
- holding of periodical meetings of the Data Protection Working Group (DPWG);
- participation of the Privacy Officer, appointed for a full-time position, with the mission to supervise the compliance of the applicable law as regards the protection of data in the framework of SWIFT'S services.

72. SWIFT considers that if the Commission should consider that a recommendation would be necessary, this would have to also take into account the initiatives described and to explicitly refer to them.

IV. THE STATUS OF SWIFT

73. The Commission opinion 37/2006 qualifies SWIFT as controller of the data processing carried out through the SWIFTNet FIN service, while considering that the financial institutions also exercise a responsibility. According to opinion 10/2006 of Group 29, SWIFT meets the definition of data controller both as regards the normal processing of personal data in the framework of its SWIFTNet FIN service and as regards the processing including a personal data transfer to the UST.[17]

74. SWIFT has disputed this status of data controller and has declared that it considered itself a processor.

75. SWIFT has maintained its position regarding its status of data processor during the recommendation procedure. In response to the conclusions of the rapporteur, SWIFT has, however, declared to recognize the interest of the statuses drawn from these conclusions, with the exception of the status regarding the processing carried out in the United States pursuant to the UST injunctions.

76. The status of SWIFT determines of course the scope of the present procedure. The issue must be subject to a new complete review considering **(1)** the arguments of SWIFT, **(2)** a more thorough knowledge of the situation (among others, further to the contacts, exchanges and collaboration that the Commission has maintained with SWIFT and the information transmitted by the latter, as well as elements and information collected at the same time from various stakeholders through searches and findings conducted by the Commission), and **(3)** possible facts subsequent to the opinions rendered.

IV.1. THE SERVICES OFFERED

77. SWIFT offer to professional clients (essentially financial institutions) various services in the form of automated services ensuring the secured and monitored transmission of financial transmission through standard formats whose syntactical structure is shared by all interconnected users, in order to only receive contents legible by each partner.

[17] Page 13 of the FR opinion.

78. Although SWIFT is not a system of book entry, compensation, funds transfer or actual settlement of a transaction, an increasing number of payment systems call upon the SWIFTNet network and the services provided by SWIFT, which further increases in light of the development of real-time settlement systems (between financial institutions). These systems require an efficient and safe automation of the entire process[18], which necessarily rely on a permanent exchange of information between all partners of the payment chain.

79. SWIFT defines its "SWIFTNet" network in its online glossary ("Glossary") as "*the SWIFT advanced IP-based messaging platform. It comprises a portfolio of services and products that enable customers to communicate mission-critical financial information and transactional data securely and reliably*".[19]

80. The use of the SWIFTNet network of course requires the use of one of the four messaging services offered by SWIFT (SWIFTNet FIN, InterAct[20], FileAct[21] and Browse). More than the network itself, it is these "generic" messaging services that each contains a portfolio of specific services (for instance the FINcopy service). In its opinion n°37/2006, the Commission had already stressed the added value offered by the SWIFTNet FIN service, and particularly the formal validation of the content of the messages and their storage in the SWIFT processing centers ("back up" service): "*the messaging service comprises, at the level of the processing centers, a formal content validation, including the presence or the correct content of data in the foreseen fields (for instance is the bank of destination mentioned?; is the currency specified?, etc.). This requires a temporary decryption of the content of the message, including as regards personal data. This decryption takes place in an automated fashion. Being a part of the messaging service, the messages are also stored in processing centers in Europe and in the United-Stated for the abovementioned 124-day period.*[22]"

81. Swift's "General Terms & Conditions"[23] define the term "*service*" as: "*any value-added service provided by SWIFT (such as the FIN or the Accord or the SWIFTSolutions) or by or for a Service Provider such as a Real Time Gross Settlement, that is accessed by Customers using SWIFT*

[18] See update of 4 May 2006 relating to "Oversight of SWIFT" on www.swift.com > about SWIFT > Governance > Oversight of SWIFT. See also the definition of the term "service" in the SWIFT "General Terms & Conditions", which refers to the activities of the compensation systems and the real-time settlement systems and includes messaging services in favor of such systems.

[19] [English original text]

[20] Aimed at constituting an environment for real-time exchange of messages.

[21] This service makes it possible to exchange any file or document through the SWIFT Network.

[22] Opinion 37/2006, p. 4.

[23] SWIFT's exhibits file (no. 3.1).

services and products" (Article 1.9). SWIFT's glossary ("Glossary") moreover constitutes an exhaustive list of the services offered by SWIFT based on generic messaging services.

82. The additional service provided probably does not add any value to the personal data themselves (except, in the framework of the process of exchange of information, the integrity value that the institution recipient of the message may attribute to them, which will then itself process these data). The additional service has not, as such, as object the processing of these personal data (such processing would only be an inevitable secondary effect of an activity pursuing other purposes). But the operations carried out on the personal data during such specific activity (whose admitted objective and added value would consist in satisfying the needs of the financial community) clearly remains subject to the Privacy Act requirements. This requires, among others, that the rights and the protection of the data subjects be guaranteed during all processing of the information that relates to them.

IV.2. DATA PROCESSING: A REVIEW OF THE FACTS

83. Article 1, §2 of the Privacy Act defines the processing as "*any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, as well as blocking, erasure or destruction personal data*".

84. One must thus identify the main operations that are performed upon the data that go through the SWIFTNet network via the services offered by SWIFT.

85. In order to determine whether these operations pertain to one or several acts of processing, it must be assessed whether they pursue only one specific purpose or whether several purposes are pursued.

86. In that respect, it must be recalled that the purpose(s) of a processing cannot be confused with general objectives that would correspond to the individual or collective good (the benefits and advantages legitimately expected), to the social goal or to the legal missions of those pursuing such objectives. But a data processing (whose scope is limited to its specific purpose) may of course

contribute to the pursuing of these general objectives[24]. In order for the processing to be legal, such participation must be necessary[25].

87. The purpose of a processing must be precisely defined, in the absence of which its necessity could never be proven. Similarly, the qualities required for the processed data could never be rigorously guaranteed, in order for the persons' rights to be effectively protected or to be effectively exercised (in particular the adequacy, the relevancy and the non-excessiveness of the data, or their exactness, which must be guaranteed with respect to the purposes for which these data are processed; or also the duration of their storage, which may not exceed the duration required to the fulfillment of such purposes)[26].

88. SWIFT describes all operations performed on the data during the use of the SWIFTNet network (in particular, in the framework of the SWIFTNet FIN service) as the elements of a single processing, different for each transfer order. This processing (the main operation) would consist in the simple transmission of the information required for the relevant international payments and for the funds transfers linked thereto, and its purpose would be the mere execution of the instructions of the payer. SWIFT declares that it limits the object of its intervention to the sole transmission of each of the messages it is entrusted with, and by reference to Recital 47 of EC Directive 95/46, describes itself as provider that limits itself to the offering of a transmission service (and is thus only the processor of the issuing banks for each of the orders that are transmitted through its service). SWIFT attached a particular status to this limited activity, which would be carried out to the benefit of the obligations of the bank, in its capacity of supposed data controller (and better than the bank itself could do it) and in accordance with the obligation imposed by the law on all processors: the securing of the processing of the carried-out transmission.

89. This reasoning taken to extremes would make it possible to consider that the true data controller is actually the payer: the bank itself would only carry out instructions given by its client. Moreover, in numerous respects, and more specifically by case-law, the bank is considered as its client's agent (general mandate for the storage and the proper management of the amounts it is entrusted with; specific mandates for the performance of decisions to use funds: the bank may only

---

[24] It does not matter that they have been determined by others than those processing the data or even that they would be evident with respect to a specific context. The generalization of the use of automated processing for financial flows is in particular considered by the financial community as a an unavoidable objective, which must be necessarily fulfilled in a society which requires technologies ensuring the extreme rapidity of the exchanges to which such flows are linked, in particular commercial transactions.

[25] Article 5 of the Privacy Act, in particular §1er, e) and f).

[26] Article 4, § 1er of the Privacy Act.

transfer the amounts determined and communicated by the client, but the latter may of course be mistaken). On the other hand and without being disputed, no one has ever inferred therefrom that each of the operations (processing) performed by the bank on the data of its client, even in execution of one of his/her orders and even if these operations are a consequence of such order, would participate in such execution only and would be carried out in the interest of the client, on his/her behalf and within the boundaries of the specific instructions that it would give in relation to the operation of processing of his/her data (independently of the instructions relating to the financial movements to be carried out), as would be required by the law if the bank were to be considered as agent or "processor" of its client for the data processing that it performs.

90. The above general considerations of course do not make it possible to assign a status to SWIFT's intervention, as regards its possible responsibility or its role of processor. They nonetheless require more details in the description and in the analysis, than SWIFT proposed in the first arguments that it has put forward.

IV.2.1. The operations that were carried out

91. The clients' data contained in the payment orders, for which the SWIFTNet network and the SWIFT services are used, undergo various operations (in the meaning of the Privacy Act), each of them possibly relating to a specific processing or constituting – together with other operations – a more general processing.

92. The most significant operations are the following, it being understood that the scope of some of them may depend on the kind of relationships between the payer's bank and the beneficiary's bank, on the more or less great variety of the SWIFT services used by these banks and on the (absence of) intervention of institutions or intermediary settlement systems:

a) collection by the bank of the order data on the basis of the information required by rules that are specific to the financial institution, to all of its correspondents, established by banking custom, or imposed on financial institutions by laws and regulations relating to the execution of funds transfer orders;

b) verification by the bank of the exactness of the collected information (validation of the reality of the constituent elements of the financial operation);

c) creation of the message by the bank on the basis of standardized structures required by the use of one of the SWIFT messaging services, and containing compulsory authenticators (identity of issuer, origin of the transmitted information);

d) transfer by the bank of the assembled data to the SWIFT network, either message by message, either by batches of messages (that are processed individually as of their entry on the network), after a first regrouping on the basis of specific criteria (for instance non-urgent messages) or on the basis of the bank's practices (transfer at fixed time);

e) all the information contained in the message is signed by the bank's system (through a private signature key that is only held by the bank, this key constituting an asymmetric key with a public key that only permits the reading and authenticating of the signature and which is available to the other partners of the bank; SWIFT only possesses the public key of its clients and users)[27];

f) first encryption of the messages by the bank's system at the time that it is sent on the network, with an encryption key automatically determined by the SWIFT processors[28] on the basis of a 'dialogue' with the bank's system, in order to guarantee its strength with respect to the environment within which it will be used (the keys are thus established specifically for each connected financial institution and based on their own system; they are systematically modified several times a day, through the same automated procedure);

g) receipt of the message by that of the two SWIFT processing centers, located respectively in the Netherlands and in the United States, to which the bank connects itself[29];

h) decryption and automated reading of each message by the regional processor of the SWIFT system[30] attributed to the bank and to which it is connected (in order to validate

---

[27] It appears from the rules of the banking practice that the bank takes on the responsibility for the message and its content by signing it.

[28] The algorithm that calculates the key is particularly secured, its performances are regularly audited and it is periodically re-evaluated.

[29] The two processing centers are active in the same way; the messages may thus arrive indifferently (as regards the rest of the operations) in one or the other center, depending on the connection(s) of the bank at stake.

[30] All SWIFT processors are physically located in the same processing center; the various regional processors are the means of entry and dialogue of the banks and the SWIFT system; the latter do not have direct connections with the central processor; the allocation of the banks between the various regional processors is not based on geographic criteria but on

the message based on the existence of the data and of the syntax required for certain fields);

i) the signatures linked to all information are verified by each participant when he/she first opens the message (upon each of the successive decryptions and encryptions), including upon receipt by the system of the recipient bank; this verification allows for the certification of the integrity of the data contained in the message and their absolute conformity with the information collected at the beginning of the process and integrated in the message by the payer's bank[31];

j) transfer of the message to the SWIFT central processor ("slice processor") where it is decrypted and encrypted with a new key, internal to the SWIFT system;

k) this centralization then allows for the orientation and regrouping of messages intended for the same recipient institution;

l) as long as the recipient institution is not connected to the SWIFT network, the messages are kept in a queuing line dedicated to each recipient within the central processor (a duplication of the messages is carried out, the copies are sent and kept in the regional processor to which the financial institution is connected); the SWIFT general terms and conditions impose at least one daily connection to system users, in order to regularly empty the queuing lines that are created; the SWIFT processors nonetheless keep the messages in queuing line for 14 days if the recipient institution does not connect itself; this "supervised deposit" is aimed at dealing with "disaster situations" to which financial institutions may be confronted and which require a temporary inactivity (natural disaster, social conflict, attack, etc.);[32]

---

criteria that are specific to SWIFT (kind of messaging service that is used; secured access; fluidity of all transfers; prevention of a risk of confusion between institutions sharing similarities etc.).

[31] The validation and verification of signatures is followed by the issuance of an acknowledgment of receipt to the issuer (this acknowledgement of receipt is a proof of treatment of a message that is correctly formatted and the integrity of which is maintained, and its delivery or its absence may trigger, depending on the kind of damage, the responsibility of SWIFT or the responsibility of the bank). The messages that are not validated or for which the information integrity is not guaranteed are subject to a message of error and refusal by SWIFT and are archived as is (for 124 days).

[32] All processes that are centralized within the various SWIFT processors moreover guarantee the uniformity of the control, of the quality of the processing (including as regards transfer time and reception rules), and of the normalization process which provides for the "translation" of the messages in a common language, ensuring the interoperability of the systems of each institution.

m) as soon as the financial institution is connected, the messages that it is meant to receive are sent, one by one, after having been decrypted (abandon of SWIFT's internal key) and encrypted once again by a key determined by SWIFT (and modified in the same way as the initial encryption key), which will be shared with the recipient's system;

n) the message will be decrypted by the recipient's system, which will carry out a last verification of the signatures, and which will read it automatically (with the certainty that it is legible, as a result of the syntactical validation carried out by SWIFT, and the certainty that the integrity of the received information is maintained) in order to allow the recipient's bank to carry out the last financial operations (and the data processing that is linked to it) executing the initial order[33];

o) the central processor carries out a duplication of the messages and of the processing and the real-time doubling of the latter ("mirroring") in the operational centre to which the bank is not connected in order to offset the potential deficiencies of the system, and then in order to regroup and temporarily archive said messages for a period of 124 days; the messages are archived in the same way in the two operational centers, in the Netherlands and in the United States;

p) the temporarily archived message and its copy are definitively destroyed after 124 days;

q) the validated messages may be automatically copied and communicated, upon instruction of the issuing bank, to a SWIFT third party client that it designates[34]; only one possibility of copy is offered[35];

r) all carried out operations are traced by a sequential numbering that is specific to each message.

---

[33] Upon request of the sender, SWIFT may confirm the delivery of the message.

[34] This liberty to opt or not for the issuance of copy and to designate the recipient thereof may appear theoretical and to constitute in practice a real constraint when the proper performance of a funds transfer operation is governed by a real-time automated interbank settlement system that requires such a copy; this constraint is, however, merely the consequence of the bank's choice to participate in the organization of financial markets in such or such a way; and, in the event such choice is itself quite conditioned, it will essentially depend on the nature of the financial markets in which each bank is an actor, and will not be, as such, linked to the use of the SWIFT system.

[35] The risks of a loose control of multiplication and diffusion of the messages and their content are thereby contained.

93. Archiving in a central and common base allows one to conduct the operations identified by the "Data Retrieval Policy" under the conditions set by the latter:

s) the recovery and restitution of the transfer data or of the data contained in the messages to the exclusive benefit, and to the motivated request, of the clients concerned;

t) the approximation and the extraction on the basis of common features of data from various messages or from series of messages that have a different origin (at least the date, as it will determine the storage duration) **(1)** to gather them in the form of statistic results and then send these anonymous results to third parties (upon request of collective organizations in order to analyze and understand certain aspects of financial flows), or **(2)** possibly to answer requests or legally binding injunctions issued by a competent authority based on applicable law and provide these data to the authority concerned;

94. Besides the commercial services offered by SWIFT, punctual operations have indeed been carried out by the company on the temporarily archived messages it possessed and the data contained in the latter, upon injunctions of the UST. These operations are considered and governed by the “Data Retrieval Policy” and have been executed in that framework. Generally, similar situations requiring operations of the same nature could arise again (both in the United States and in Europe). The scope of the operations and their particularity will of course depend on the scope, the particularity and the binding force of the act of the acting authority, and of the powers of the latter. However, it appears useful to specifically describe the operations carried out to comply with the UST injunctions, in order to later examine what they may possibly determine in relation to SWIFT's status. These operations have consisted in:

u) the selection, regrouping and extraction of copies of archived messages on the basis of common features (in the specific case of the UST injunctions, only dates, country of origin or of destination, and certain categories of standard messages[36]);

v) the duplication of these messages and their content;

w) the communication of copies to the UST.

[36] For the FIN messaging system, there are about 250 different categories of standard messages; the UST injunctions only applied to some of them, specifically determined and identified in each injunction.

95. Two elements should be stressed and be subject to specific attention:

- SWIFT messages are structured in two parts: the envelop and the content; the envelop, as opposed to the content, only contains non-identifying data (essentially the standardized data of the institution that issues the message and those of the recipient institution(s)) and the information of the envelop are the only ones exploited by SWIFT, in order to organize the succession of operations and the orientation of the messages; it is certain that SWIFT does not exploit the identifying data of the data subjects and does moreover not possess the tool that would allow it to directly access the identifying data contained in the messages that it keeps; the identifying data[37] contained in the messages are indeed subject to a processing carried out by SWIFT (encryption, decryption, automatic reading in order to certify their integrity and in order to certify the integrity of their link with the accompanying data, storage, destruction, etc.) but they are not exploited by the company, nor for the orientation of messages, nor for their regrouping, nor for their potential retrieval from archiving, nor even for the creation of statistics;
- the two SWIFT processing centers are fully active; contrary to what may have been said, all processed data are not initially concentrated in the processing center in the Netherlands to be later transferred to the U.S. center; the processed data, which are all subject to an international transfer to the center that has not received them, have thus, upon such transfer and for some of them, a European origin, for some others a U.S. origin.

96. Finally, it should be recalled that the response given to the communication of archived messages to the UST was made in a particular framework. The Board of Directors of SWIFT considered that the reach of the injunctions that followed the one made after September 11, 2001 was disproportionate and that they could be affected by a lack of legality; it forwarded to the U.S. administration the decision to submit the question to a court in the event that these requests were maintained as is. The same board then admitted the obligation to comply, without any objection or appeal, with the subsequent injunctions, otherwise formulated and supervised, by considering on the basis of detailed analysis that it no longer had arguments to raise before a court as regards the excessive scope and thus the legality of the requests.

97. In response to the objections initially formulated by the Board of Directors of SWIFT, the UST has established the terms applicable to the transfer, by limiting the exploitation of the transferred data to processing that could be considered as “legitimate” (fight against terrorism

[37]That is the data that directly or indirectly, but exclusively, identify the data subject and which grant the status of personal data to the information to which they are connected: in the SWIFT messages, this essentially covers the name, address, account number, etc.

financing, such term being defined pursuant to international conventions, in the framework of and following legal procedures) and “fair” (retrieval of the data on the basis of prior indications in order to avoid an abusive and systematic consulting of all transferred data). These terms were established in a "Memorandum of Understanding" binding on the U.S. administration. SWIFT moreover obtained a "comfort letter" from the U.S. administration to its benefit (and not to the benefit of the individual clients of SWIFT).

98. SWIFT obtained the power to ensure itself that the transferred data would not subsequently be processed in a way that would be incompatible with the purposes for which they had been transferred. Thereby, well before the publication of the UST “Representations”, SWIFT obtained that scrutinizers could carry out a 24/7, on-the-spot, control as regards the way the UST processed the available data in the United States. The “Representations” refer to this in very explicit terms: "*SWIFT and outside auditors it has retained exercise their independent oversight over the TFTP (Terrorist Finance Tracking Program) in several mutually complementary ways. First, certain SWIFT representatives have been granted appropriate security clearance to have 24-hour access to the equipment and data and the ability to monitor, in real time and retrospectively, the use of the data to ensure that they are accessed only for counter terrorism purposes. Additionally, these SWIFT representatives may stop any specific search immediately, and even have the ability to shut down the entire system, if they have any concerns*".

99. In response to the objections raised by SWIFT, the UST has moreover undertaken that the information revealed by the retrieved data (on the basis of prior indications) would only serve itself as indication and would be subject to a confirmation by other sources prior to exploitation in a procedure[38].

IV.2.2. Essential means: standardization

100. The definition of standards ("SWIFTStandards") and their shared use for the exchange of financial messages and the performance of services linked to the exchange[39] constitute an essential characteristic of the services that SWIFT offers to the financial sector. SWIFT’s 2007 annual report stresses that: "*Standards are the heart of SWIFT's value proposition*".[40]

---

[38] The most natural of these sources being the financial institutions concerned with the transaction, these being bound in most states by strict obligations of information and of collaboration with the authorities as regards fight against terrorism financing. The confirmations, for the institutions located outside the United States, required thus collaboration with the police or judicial authorities of the relevant States (without such authorities being necessarily or formally informed of the origin of the information that is transmitted to them).

[39] www.swift.com > Standards.

[40] SWIFT annual report 2007, p. 6.

101. SWIFT describes these standards as "*an agreed way to do things*", and the SWIFTStandards as "*the overarching name for standards products, tools and services that SWIFT delivers to the SWIFT Community*"[41]. The standards establish common formats and a common syntax of content for all “tools” materializing the performance of the various offered services. Such common language opens of course many possibilities of interaction, simplified exchanges, validation through a single procedure and a single intermediary, syntactic corrections or tracking of syntactic mistakes by the “language master”, which is the intermediary in the communication process.

102. Several standard types are used during the exchange of information, through SWIFT’s messaging services. A first variant structures the various categories of MT messages ("Message Type") for the use of the FIN service. Another variant uses messages’ structures in an open format (XML). Other standards have been developed, for which one of the imperatives was to comply with the requirements of the ISO standards, either ISO15022 standard, either ISO20022 standard (or UNIFI for "UNIversal Financial Industry message scheme"). The standards for payment messages imposed by SEPA (Single Euro Payments Area) in Europe will have to comply with the ISO20022 standard. When SWIFT processes an ISO20022 message through its network, it refers to it as an “MX” message. MX messages may be processed through the FileAct and InterAct services.

103. It must be stressed that SWIFT was appointed as "ISO Registration Authority" for the registration and approval of the ISO15022 and ISO20022 message standards.

IV.2.3. The purposes

104. The review of the operations identified supra and of their context allows for the formulation of several remarks regarding the determination of the processing carried out and of its purposes.

105. It appears incorrect to describe the chain of operations as a single transmission processing, specific to each message. The information linked to each order is not only the object of a simple transmission through a messaging system, but it is also subject to requirements (in terms of form and content) and to operations that are identical and common to all messages.

106. The operations carried out on the data of each message may also not be justified (or at least exclusively justified) by the need to ensure security and confidentiality of the personal data

[41] "Glossary", annex 3 to the response of 16 November 2007 to the written questions of the Commission.

that these messages contain during their transfer. One may certainly not ascribe this objective to the operations carried out in a centralized way that rely on the indispensable use of shared means (common standardized language).

107. In that respect, it must be underlined that, to the question "Why can SWIFT not apply an end-to-end encryption to the personal data processing via its network in order to ensure that only banks may access these data", SWIFT responds: *"SWIFT clients require a centralized encryption. A through and through encryption of the data would indeed prevent SWIFT from conducting the validation of the fields of the messages that is required in a centralized way by its clients. (…) The decentralization of the encryption would imply (…) a questioning of the system's uniformity. (…) SWIFT clients have repeated their will to maintain a centralized validation, this validation being considered as an inherent and indispensable feature of the SWIFTNet FIN service*." SWIFT also indicates that the decentralization of the encryption "*would also affect the security of the operations, as SWIFT would no longer be able to guarantee the back-up of the messages, whose access would be rendered impossible further to the loss of the encryption keys*"[42].

108. It therefore appears that the transmission of messages is not the only object of the SWIFTNet FIN service, but that the latter has as essential feature ("inherent and indispensable") the validation of the fields of the messages. The service also guarantees "the security of the operations" at a level which each bank (and thus each processor in its individual relationship with the data controller that instructs him) could not achieve. Without event ruling on the status of SWIFT, one may already conclude that Recital 47 of Directive 95/46 CE may obviously not be invoked to determine the status of SWIFT (see *supra* point 88).[43]

109. One may obviously conclude that the processing carried out by SWIFT and by the financial institutions when they use the SWIFT services to contribute to the furthering of this objective have at least as specific purposes (each linked to one or more processing operations): **(1)** the transmission of financial information; **(2)** the authentication of the issuing bank; **(3)** the certification of the integrity of message data; **(4)** the guarantee of the legibility of the message and of the immediate exploitability of the information they contain for all institutions concerned (including through the validation of the presence of compulsory information in certain fields and of the adequacy of the syntactical expression); **(5)** the real-time communication of the information of the

[42] SWIFT response dated 16 November 2007 (point 1.6) to the written questions of the Commission.

[43] "47 - *Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services*; (…)".

validated message (by the automated production of a copy) to designated third party operators, for instance, with a view to contributing to the proper performance of the operation (settlement platform, central bank for recording in the accounting books, settlement institution...), **(6)** the a posteriori certification and the evidence of all operations carried out by the various participants (issuing bank, SWIFT, recipient bank) on each message, and **(7)** the compensation of the shortcomings, including those of the IT systems of the financial institutions but also those that are linked to forced or predictable periods of inactivity of these institutions (through tracking, mirroring, temporary storage and temporary archiving for 124 days), etc.

110. If an objective of security does indeed exist, which includes - among others - the procedures of authentication, validation and certification, it is essentially and more accurately the safety of the financial operations themselves that is at stake (the capacity to execute transactions with as little risk as possible), in an economic context that implies cross relationships between multiple financial institutions, with references and functioning rules that are quite different, and that requires an ever-increasing rapidity and even an immediate processing of this kind of operations. This relates - among others – to the correspondence of the supporting financial operations to the rapidity of commercial operations, while guaranteeing to each partner that the exchanged information is understandable, legible and integer (and thus immediately exploitable).

111. The standardization of information in a common “language” offers the certainty that the cross orders from the various financial institutions may be processed in the same way and within the same deadlines and that all financial institutions will be able to be interconnected on the basis of common and undisputable exchange rules. This double guarantee appears particularly important when real time gross settlement systems and the automation of all interventions within the chain of payment tend to become the rule, to ensure both rapidity of operations and stability of the markets[44]. The interconnection and the controlled standardization of the procedures and the information are of course indispensable to benefit from real-time irrevocable transfers[45].

---

[44] The ability to immediately execute an international financial transaction makes it possible to avoid the risk of “systemic choc” for the markets. This risk exists when transactions between banks are simply entered into the books as and when the information is transmitted and that financial transfers are carried out once a day, upon closing of the account; it is then possible that a bank has given transfer orders for amounts larger than these reserves and cannot honor its dues. Real time settlement makes it possible to permanently receive insurance as regards the reserves of the issuing bank, during each transaction or series of transactions, and to immediately increase the available reserves of the recipient bank (which may thus immediately cover new transactions).

[45] It must also be noted that settlement mechanisms for the entire euro zone, TARGET 1 (*Trans European Automated Real Gross Settlement Express Transfer*) and now TARGET 2 are ensured by the interconnection of banks (*Interlinking*) via the SWIFTNet network and the use of SWIFT services, procedures and standards. The conditions of such use are, however, external to SWIFT and are set by the rules and the framework determined by central banks. SWIFT is also mentioned as the reference intermediary on the SEPA (*Single Euro Payments Area*) website and in the European Payments Council documents.

112. In light of the above elements, it appears that one of the central objectives of SWIFT is to provide a response to collective needs of the financial markets (rapidity, stability, safety of financial operations, harmonization of exchanges, etc.).

113. It is in this context that financial authorities, and among others the Belgian National Bank, have been able to affirm that SWIFT's intervention guarantees worldwide financial stability[46]. SWIFT repeats this affirmation[47].

114. A purpose generic to various data processing carried out by SWIFT or via the use of SWIFT services clearly appears, which could encompass the purposes more specifically identified under point 109. One could define it as: contribution to the safety of financial transactions through the automated and secured transmission of information which are standardized, for which the integrity is maintained and which are directly exploitable[48].

115. In a non-systematic fashion, in the framework of the collective requests envisaged by the "Data Retrieval Policy", SWIFT carries out the retrieval of the non-identifying data (transferred amounts, currencies used, dates, origin, destination, etc.) that are separated from the identifying data of the message of origin, and thus completely anonymized, in order to regroup them as statistic values or as general information linked to the financial messaging service, for collective entities and in the framework of studies or analysis of financial markets. The clear purpose may in this case be defined as follows: the production of general information on financial transactions.

116. It is also important to precisely determine which is or which are the processing purpose(s) carried out by SWIFT in the framework of legal requests or injunctions as contemplated in the "Data Retrieval Policy". Generally, it must be underlined that SWIFT has had for more than 15 years, through this policy, rules that will allow it to determine and develop a policy specific to this kind of situations, and thus to carry out possible data processing in that framework.

---

[46] See BNB report, "Financial Stability Review", 2005.

[47] SWIFT exhibit files nos 2.2 and 2.3 (work documents of 7 September 2006 and response of 7 November 2006 to opinion 37/2006 of the Commission).

[48] It being understood that the operations carried out by SWIFT are not sufficient to secure transactions and markets and that SWIFT's intervention has, as such, no effect on the transactions. It is the transaction's partners that make all decisions; but in the organization of international markets, SWIFT's intervention (or the intervention of a similar system) is necessary for them in order to decide. It being understood that it is the safety of all transactions that is each time at stake, and not the safety of each considered individually: indeed, the safety of an executed transaction may guarantee the proper performance of a future transfer (see note 41).

117. In abstracto, and while considering the binding nature of the injunctions and the requests that would be addressed to SWIFT, should one also consider that the processing purpose(s) in that framework would correspond with the objectives pursued by the authors of the obligation[49]? This hypothesis does not conform to the Privacy Act, which clearly differentiates between the legal obligation, the data processing required by this obligation and the responsibility for the processing. In truth, it appears that this kind of obligation frequently aims at another result than the processing itself, and that the way it is carried out by its recipient is not relevant to its author. The latter does not impose one specific processing or another, but a result. Among the five legal grounds authorizing personal data processing, the law indeed foresees the processing "necessary to comply with an obligation binding on the data controller based on a law, a decree or an order"[50].

118. It must be concluded that the most general purpose that can be assigned to this processing, is: performance of the legal obligation (Belgian, U.S. or other, depending on the originator's status and the applicable law) that applies to the data controller, without this actually giving more indications on the identity of the data controller (see infra – IV.3.4.).

IV.2.4. Determination of the purposes and means employed

119. SWIFT bases a large part of its argumentation on its absence of power and of capacity to determine the specific processing purpose and means that it would carry out for the account of each of the client banks on the basis of the instructions that each of them would specifically provide for each message concerned, namely the transport of the message through the supply of a simple messaging service.

(A) Scope of the law

120. To formally and legally establish who the data controller is for a processing of personal data, one must actually identify the one determining the purposes and the means of the processing[51]. The processor, on the other hand, is the one processing the data on behalf of the data controller[52], it being understood that it may only act upon the sole instruction of the data controller[53].

---

[49] This hypothesis would lead to designate, without any further review, the UST as data controller of the conducted processing.

[50] Article 5, § 1, c) of the Privacy Act.

[51] Article 1, § 4 of the Privacy Act.

[52] Article 1, § 5 of the Privacy Act.

[53] Article 16, § 1, 4° of the Privacy Act.

121. Therefore, logically, any given intervention for the account of an instructing beneficiary does not allow the one invoking the capacity of processor in the meaning of the Privacy Act to decide on data processing (physical operation) by which means the instruction will be carried out (purpose), nor on the means to be employed to carry out this operation. The relationship between the data controller and the processor revolves around the processing itself, and not around a third operation (be it an event necessary to the apparition of the data that will be processed and would it condition the future processing of this data).

122. To establish who determines the purpose and the means of each identified processing, it is therefore not relevant that institutions or groups (here banks and more generally financial markets) have notified one or more needs. The question is to know who decides that it will be such specific processing (physical operation), having such purpose, carried out in such way (technical features) and in such conditions (general means, including organizational) that will satisfy or help satisfy this need.

123. The responsibility of a processing requires at least the ability to control (be it intellectually) all processed data or at least all data subject to a common automated processing likely to bring them closer, and an ability to control the processes applicable to all this data.

- **Contractual qualifications are not decisive**

124. The definition of data controller under Article 1, §4 of the Privacy Act is a mandatory legal provision. If the designation of a party as data controller or processor in a contract may reveal relevant information regarding the legal status of this party, such contractual designation is nonetheless not decisive in determining its actual status. Such status must be based on concrete circumstances.

125. Moreover, the criterion of “the author of the collection” or of the initial collection retained by SWIFT in its policies to determine the initial process of a processing chain that would be attributable to a single controller, is not a relevant criterion. This criterion does not appear in the legal definition of data controller. Two conditions are required to assume the responsibility of a processing, but they are sufficient: determine the purposes and the means of the processing. The Privacy Act moreover considers the cases of processing of data that the data controller has obtained indirectly or that have been communicated to it through the controller of a previous processing.

- **The concept of processor has a specific definition based on the Privacy Act and cannot be interpreted based on external legal sources**

126. The concept of processor, defined under Article 1, §5 of the Privacy Act is frequently confused with the everyday meaning of the term, as it can be interpreted outside the application of the Privacy Act. Certain financial institutions for instance refer to circular PPB 2004/5 of the BFIC that explicitly qualifies SWIFT as a processor. This status has of course not been established in application of the Privacy Act and the criteria that it uses, but based on other legal areas that are relevant to the competence of the BFIC.

(B) The decision-making process as regards SWIFT's interventions

127. SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) is a cooperative society organized under Belgian law, based in La Hulpe, close to Brussels. It was founded in 1973 by 239 banks from 15 countries.

128. On September 30, 2007, SWIFT had a total of 8551 clients, the "SWIFT Users that, together, constitute the "SWIFT Community"[54]. These 8551 clients are divided in four categories, the first three covering 7788 financial institutions: **(1)** 2292 cooperating shareholders ("Members"), **(2)** 3254 subsidiaries or branches of its cooperating shareholders ("Sub-Members"), **(3)** 2242 members that do not own shares ("Non-Shareholding Members") and finally **(4)** 763 clients that are not shareholders nor financial institutions.

129. In the introduction of its 2007 annual report: "Community inspired", SWIFT indicates that: "*We act as the catalyst that brings the financial community together to work collaboratively to shape market practice, define standards and consider solutions to issues of mutual concern and interest*"[55]. SWIFT indicates on numerous occasions that it is structured by a community logic.

130. SWIFT's shareholding is determined by the use of the basis messaging services that the company provides. The more or less large use of the services determines the size of the shares held

[54] Point 2.8. of SWIFT's questionnaire, mentioned in annex to the letter draft on behalf of SWIFT on 16 November 2007.

[55] "Community Inspired", SWIFT Annual Report 2007, p. 1.

by each client (as of a minimal level of use). The shares are redistributed on that basis every three years[56].

131. The composition of the Board of Directors of the company also expresses such a participative logic. The Board is composed of 25 members. They are appointed for a renewable 3 year term upon proposal of the groups of national members depending on the number of shares held by all members of the relevant country: the shareholders of the six countries holding most of the shares collectively suggest two directors per country; the shareholders of the following ten countries suggest collectively one director per country; the other members may suggest three directors by joining forces with the members of other countries.

132. The directors must necessarily come from the financial institutions members of SWIFT, where they continue to carry out their duties. They are not paid by SWIFT. The employer of the President of the Board of Directors is reimbursed of the part of salary corresponding to the time spent in performing its term[57].

133. In its response of November 16, 2007 to the written question of the Commission[58], SWIFT details what it presents as the decision-making structure within the cooperative company. Several documents previously communicated and the information collected by the Commission detail such functioning. SWIFT's "Corporate Rules" establish contractually the process described and the role of the various actors that take a part in the important operational decisions[59].

- **First level: national users groups and national member groups**

134. The institutions client and possibly cooperating of SWIFT, each of them individually, are associated with a users group and, for the cooperating entities, to a national members group. These

---

[56] "*The Company manages the units through the reallocation principle defined in the by-laws and in the General Membership rules. The units held bye ach member are proportional to the annual contribution paid bye ach member for the network-based services of the Company. The exact number of units allocated toe ach member is determined at least every three years by the Board of Directors, and the members have the obligation to give up or take up the resulting change in units. The by-laws state that units are only reimbursed when a member resigns or when a member has to give up units following a reallocation*". SWIFT Annual Report 2007, p.57

[57] For the list, the national origin and the institutional affiliation of the current directors: SWIFT Annual Report 2007, pp. 32-33.

[58] Point 3 of the response of 16 November 2007 to the written questions of the Commission.

[59] "Corporate Rules" of SWIFT, attached to the response of 16 November 2007 to the written questions of the Commission (annex 5). Available for consultation on www.swift.com > About SWIFT > Governance > Corporate Rules.

groups constitute the first level of review of the important issues linked to SWIFT's activities and to the services that the company provides or could provide. Each institution is responsible for its (non-) participation in such groups. SWIFT's "Corporate Rules" indicate that these users group are independent from the legal structure and from the decision-making bodies of SWIFT[60]. These groups do not formally possess the decision-making power.

135. The national users groups constitute a discussion forum for operational and technical questions linked to the use of the service provided by SWIFT. They also fulfill the role of evaluation tool and indicators for the Board of directors, through which the "*community of SWIFT's users (SWIFT Community) report their needs and demands*"[61].

136. The national members groups may give their opinion on questions that are likely to affect the members in such capacity (terms of allocation of the shares, value of the shares, creation of a new category of users, etc.). They also help "*coordinating the points of view of the various members and permitting the adoption of common policies*"[62]. They nominate the candidate directors, but one may say that, in fact, they appoint them (the members of the Board of Directors being divided by country – see supra). Moreover, the members give in any event their opinion as associates sitting at the general assembly.

- **Second level: the committees instituted by the Board of directors, the *ad hoc* working groups and the accompaniment of technical development**

137. SWIFT's Board of Directors has established six committees ("Board Committees")[63] and various sub-committees in charge of the preparation of decisions, in order to assist the bodies to which they will be submitted and that have the capacity to adopt them. Such preparatory work is, among others, aimed at synthesizing and harmonizing the results of the debates coming from the national groups[64].

---

[60] Articles 3.4 and 3.5. of the "Corporate Rules": "The National [User or Member] Group is independent from the SWIFT legal and governance structure and can organize as it thinks appropriate".

[61] Point 3 of the SWIFT questionnaire, mentioned in the annex to the letter drafted in SWIFT's name on 16 November 2007.

[62] Point 3 (Introduction) of the response of 16 November 2007 to the written questions of the Commission.

[63] The committees mentioned as relevant on behalf of SWIFT are the "Technology & Production Committee", the "Standards Committee" and the "Banking & Payments/Securities Committees".

[64] Points 1.7. in fine, 2.1. and 3 of SWIFT's questionnaire, mentioned in the annex to the letter drafted on behalf of SWIFT of 16 November 2007.

138. Two ad hoc working groups have been established by the Board of directors. A first working group, called the "Data Privacy Working Group" or "DPWG", was created in December 2006. Its mission was to formulate proposals to respond to the objections formulated by the Commission and by Group 29, and in particular to issue proposals as regards the adherence to the Safe Harbor. A second working group has been assigned the task to propose adaptations to the architecture of SWIFT (the "Re-architecture Board Task Force" or "RBTF"). These groups are predominantly composed of “representatives of the financial community”.

139. More specifically, as regards the development of standards and technical processes, a series of steps and interventions can be clearly identified:

- identification of a collective need, generally by a manifestation of any form of one or more users or categories of users;

- precise definition of the imperatives to be met and of the technical solutions to satisfy the need (business model and logical model); the *business* and *logical models* are developed by SWIFT with the accompaniment of a “modeling group” composed of technical experts of the specific field for which the standard project is being developed; this work is itself accompanied and validated by a "business validation group" that is also composed of experts of the financial institutions;

- presentation of the project to all client users, which express themselves, among others, by means of a vote (whose result is reported to SWIFT on a country basis, and weighted based on the positive and negative votes expressed within the national groups) in order to assess the more or less large adherence generated by the project;

- possible continuation of the development of the project if it appears that the largest consensus is not achieved;

- formal decision-making on the basis of the observation that the largest consensus of all client users is achieved.

140. The most important contractual provisions set forth in SWIFT’s policies are developed according to similar procedures.

- **The decision-making**

141. It is the Board of Directors that makes all actual decisions regarding the technical development and the contractual provisions of the policies. But it is unquestionable that decisions are the product of a community logic and that, as the Commission has been able to observe the functioning of the company, there is no decisions that would go or that would have gone against the largest community consensus.

142. It is more than a mere consultation of clientele (which would in any event be part of a good commercial logic), as the clientele also controls the company's bodies in order to ensure that the will that was expressed within external and independent structures are duly observed and carried out. For such kinds of decision, it is the clientele that expresses itself but that also truly makes the decision, collectively.

143. One may affirm that this constitutes an operation of mutualization of the solutions aimed at satisfying common needs. The company SWIFT is the ultimate expression of such operation. But it is not the sole vector or instrument thereof. It is not SWIFT that materializes the existence of the financial community and that would thus constitute such community[65]. SWIFT is not the financial community of its client users[66].

144. There is no constituent instrument for such community. But the facts that are described make it possible to note the existence of a true community of interest, tacitly and informally constituted, active and whose collective functioning rules are established, implemented and complied with for more than 30 years.

145. If such community of interest is not formally established, there are nonetheless, among the elements that confirm its existence, legal instruments of Belgian law (and of Belgian law only):

- the functioning rules of SWIFT and the internal acts that organize the decision-making process and that recognize its result, further to these rules;
- the various contractual policies of SWIFT, certain provisions of which established the decision-making process described above but that are most of all common to all SWIFT users.

---

[65] Even within the limit of a community that would have only been constituted for the sole objective of putting in common the needs to which SWIFT fulfils.

[66] As it has been shown, the community and its members do not express themselves and do not make decisions within the framework of an organ of the company that would gather them for that purpose (by hypothesis, the general assembly).

146. It is significant (as well as exceptional) that certain rules organizing the decision-making relating to the great orientations and achievements of SWIFT are established and confirmed by contractual provisions binding the company to its client users[67].

147. It is difficult to consider SWIFT as an entity independent from the community of its users, to the extent that the company has been created in the framework of the latter, that the use of SWIFT services is the way to adhere to it and that SWIFT expresses the collective will. SWIFT would not exist without the community of its users. But, in reality, this community would not exist without SWIFT.

148. Without having the same prerogatives as the financial institutions that constitute the community of users of the company, SWIFT may be considered as an entity bound by essence to the community, with a specific status and limited but clearly determined powers.

149. In truth, SWIFT, through its bodies, is the warrantor, the clerk and the executor of the decisions of the financial community that has gathered around common stakes and needs. One may consider that SWIFT expresses and materializes the decisions of said community and acts by being invested of a true factual delegation.

150. Moreover, it clearly appears that one or more of SWIFT's clients could not impose solutions or specific requirements deemed as marginal by the users' community. SWIFT does not devise and does not have the mission to devise, upon request, custom-built solutions for certain clients. But nothing would prevent such clients from having such solutions devised otherwise: the "community affiliation" is not exclusive, nor is it definitive; it does not imply the relinquishment of the independence of each of the members of the community.

151. It must be stressed that certain decisions made by SWIFT's Board of directors, and that imply personal data processing, are not subject to the large collective and community decision-making process. Such decisions are made in the framework of the provisions of the "Data retrieval policy" as regards the retrieval and aggregation for statistical purposes and as regards retrieval and communication further to legal requests or injunctions from public authorities. These decisions are each time subject to an assessment of the Board of Directors and may require the development of specific technical tools, in order to carry them out[68].

---

[67] In particular the "Corporate Rules".

[68] The decision to retrieve from temporary archiving and to communicate to the relevant client, upon request and to his/her benefit, the copy of a message, which the client sent or had received may, however, only be subject to a marginal assessment, which consists in verifying that the request does indeed correspond to the specific situations in which the

(C) The central role of SWIFT and the autonomy of the banks

152. The use of SWIFT's services appears difficult to avoid for certain financial operations: sending of international messages relating to transactions of urgent nature, of great value or having a high risk potential; transmission of financial information in the framework of a transaction that is accompanied by an automated real-time settlement.

153. It moreover appears that SWIFT's intervention not only takes place on behalf of the payer or of its bank, but that the processing carried out by SWIFT is also carried out to the benefit of the recipient (and thus on its behalf, as it gives effect to the authentication, the certification and the validation carried out by SWIFT), and also to the benefit of the entire financial community (and of those that have an interest in the stability of financial markets).

154. SWIFT takes on and claims this role of trusted third party or certifying third party between the partners of a financial transaction.

155. The importance of the services and of the intervention of SWIFT in such markets is confirmed by SWIFT and by the Belgian National Bank[69] when they declare that SWIFT has been placed under the surveillance of the G10 central banks in light of its "*critical importance for the proper functioning of the entire financial system, in its role of dominant provider of messaging and processing services, in particular, for the discharge of payment and share transactions*."

156. One may, however, not infer from such a situation that the banks, individually, have lost all autonomy and are necessarily subject to a kind of monopoly that would be exercised by SWIFT and that would deprive them of any decision-making power. In truth, it is not a "monopoly" of SWIFT that would lead the banks to use the services provided by the company but rather the nature itself of international financial transactions between several partners, and the need for common rules between as many of them as possible (as the financial effects of each financial transaction add up or influence one another, even if individually each of them relates to different partners).

157. The use of SWIFT's services is not compulsory and pertains to the bank's decision to integrate or not the market dynamic set up by SWIFT client users. The banking institutions remain

---

applicants would be placed and which are described in the "Data Retrieval Policy"; the determination of such situations has been subject to a large consultation process of the financial community of the client users.

[69] BNB, Financial Stability review 2005 (page 13): "*However, given the systemic importance of SWIFT for the global payment system, the central banks of the Group of Ten (G10) have considered that SWIFT should be subject to a surveillance concerted between the central banks*". This document is available at the address http://www.bnb.be/doc/ts/Publications/FSR/FSR_2005_FR.pdf

moreover free to select the way the international payment orders are carried out, subject to the agreement of the financial institution partner to the transaction. The banking institution may decide to circulate the data through its own network (international “on-us” transaction between two banks of the same group, possibly via a VPN[70], via another provider of financial services (processing via SIANet, BT/Radianz, VISA, MasterCard, etc.) or via a simple telecom operator (by fax, e-mail, etc.).

IV.3. THE RESPONSIBILITY FOR DATA PROCESSING PERFORMED BY SWIFT

Distinct classifications and responsibilities for the various processing of personal data performed on the occasion of the transmission of financial information through SWIFT’S services

158. The observation and the description of the facts allow designating more accurately the data controllers responsible for the various data processing performed. For that purpose, one must obviously take into account the fact that the data controller must keep the command, at least the intellectual command, of both the processing and the data processed, and that the processing may of course not exceed what the alleged data controller is able to master or what it would theoretically have been able to perform, assuming that it has had the means to do it or that it has chosen to rally such means.

IV.3.1. The responsibility of each financial institution

159. The bank of each payer must be considered as being a data controller (and holder of the obligations related thereto) where the individual and specific aspects of each order prevail: data gathering (and verification of their accuracy); creation of the message in accordance with the standardized structures, the legal obligations and the payer’s instructions; transfer to SWIFT’s network; first encryption (whose key is established by SWIFT, but on the basis of the bank’s system, and which is performed by said bank’s system); transfer of copies of the message, for instance to an automated payment platform; transfer of the information contained in the message to the recipient‘s bank.

160. For that matter, one should note that EC Regulation 1781/2006 of November 15, 2006 "on information on the payer accompanying transfers of funds" requires the payer’s financial service supplier to verify the identity of the payer, to supplement the money transfer order by data allowing

[70] Virtual Private Network.

for its identification and to retain these data for five years. According to Article 1, § 4 al. 2 of the Privacy Act, these provisions obviously designate the payer's bank as being data controller responsible for these various processing[71]. Besides, the message services suppliers are clearly excluded from the scope of the abovementioned Regulation[72].

161. In addition, the creation of queuing lines specific to each recipient's bank results from decisions of each of these banks (connection time and periods to SWIFT's network). These queuing lines, as well as the last decryption and the subsequent processing of the message data designed to lead the financial transaction to an end, obviously result from the recipient's bank responsibility.

162. Finally, it must be considered that the retrieval and the production of a copy of a message archived at its sender's request or at one of its recipient's request pertain obviously to the requester's responsibility, to the extent that the archiving system has been conceived with a view to producing back-up copies for potential applicants in case of need, that these are messages that are known to the applicants, that they have the capacity to access the archiving themselves to directly retrieve their messages and that the intervention of SWIFT is limited to offsetting the potential deficiencies of the system of an institution when it attempts to access the archived messages that it may retrieve.

IV.3.2. The responsibility of the financial community of SWIFT client users

163. The financial community of SWIFT client users may obviously be considered as data controller responsible for the common processing applied to all messages (or to each category of messages according to the service used) which pass through the SWIFTNet network.

164. More precisely, the financial community of SWIFT client users may be considered as controller for the following processing: decryption and reading of the messages with a view to authenticating, validating (presence of mandatory contents and readability of the message) and certificating their integrity; re-encryption (with an internal key) and new decryption with a view to performing a last encryption with a key provided to the recipient's bank; duplication and transfer to

---

[71] "When the purposes and the means of the processing are determined by or pursuant to a law, a decree or an order, the data controller is the natural person, the company, the association *de facto* or the public administration designed as being the data controller by or pursuant to a law, a decree or an order".

[72] See recital (8) of EC Regulation 1781/2006.

the processing center located in the United States and mirror processing of the whole process; archiving during 124 days in the two processing centers; destruction of the archived copies after 124 days.

IV.3.3. The responsibility of the company SWIFT

165. The company SWIFT, as such, may obviously be considered as being data controller of the processing which, on the basis of particular requests, it performs on the data or a part of the data temporarily archived, for purposes which are not directly linked to the performance of financial transactions: the selection, the connection and the extraction on the basis of common characteristics shared by different message data or series of message data which have a different origin to incorporate them under the form of statistical results and communicate these anonymous results to third parties (at collective organizations' request in order to analyze and understand certain aspects of financial flows). It must be underlined that the archiving system has not been conceived to respond to such requests. The opportunity of archiving which makes these last processing possible provides SWIFT with a marginal responsibility, however complete and autonomous, characterized by a true discretion.

IV.3.4. The specific case of processing performed in response to a binding administrative or judicial injunction

- **The impossibility of a "generic" status and the need for a status based on a case-by-case assessment of each situation**

166. The injunctions and binding administrative or judicial requests can be of very diverse nature and content, depending on the extent of the authority of their originator, the precision of their content, their objective, the more or less great latitude of execution they leave to their recipient, the existence or not of appeal possibilities allowing to challenge or request confirmation etc. There is obviously a big difference between an obligation to process data imposed by law in a precise way and a legal obligation that leaves the choice of the processing to be implemented in order to comply, or between these obligations and an injunction issued by an authority in application of the law and which could in turn hold the obligation to carry out a specific processing or simply to communicate an information while leaving the recipient the choice of the means to be used thereto. A status under the criteria of the Privacy Act will only be possible to establish taking into account all the

specificities of each situation. The recipient of an injunction may be responsible for the way in which he executes this injunction just as much as he may be left without any option to choose.

- **The specific case of the data transfers to respond to the binding injunctions of the UST**

167. It does not appear relevant to search for a qualification of the processing carried out by SWIFT in the U.S. on data localized physically in this country in order to respond to the binding injunctions of a U.S. authority. In any case Belgian law does not apply on U.S. territory, and any qualification would remain purely theoretical and without effect: none of the obligations of Belgian law could be imposed on this ground.

168. This situation may, however, have been a source of ambiguity, SWIFT acting in two distinct capacities: in the U.S. as recipient of the injunctions from the UST and in Europe as operator of a data transfer to a third country. For each of these capacities, SWIFT is subject to a different legislation.

169. It is evident that acting as an operator of a transfer to third country, SWIFT could not ignore the changes in the level of protection of which the transferred data benefited (contrary to what may have happened if the data had been transferred to a third party company). It is in this capacity, and only in this capacity, that SWIFT was bound to act in the opinion of the Commission. It is only in this capacity that the attitude of the company should be considered, without regard to hypothetical obligations that would result from the Privacy Act following a qualification deriving from a situation subject to U.S. law.

V. THE MEASURES ADOPTED BY SWIFT

170. In the course of the year preceding the beginning of this procedure, the Commission maintained a regular dialogue with SWIFT through detailed letters and multiple meetings[73], some of which in the presence of representatives of Group 29 and of the European Data Protection Supervisor (EDPS). The continuation of the dialogue with SWIFT had, among others, as purpose to encourage the latter to develop a new personal data protection policy that, by conforming to the aforementioned opinions, would better take the relevant European and Belgian regulations into account.

171. Indeed, since the adoption of the Commission's opinion 37/2006, SWIFT has adopted various measures aimed at better safeguarding the protection of personal data processed in the framework of the services it provides. This covers, among others, the development and adoption of new contractual policies ("policies") relating to privacy protection, the adherence to the "Safe Harbor Principles" to supervise the processing carried out on the U.S. territory, the decision to modify the architecture of its network and the publication and circulation of information specific to processing carried out in the framework of its activities, designed both for financial institutions and the public.

- **New policies regarding personal data protection**

172. Further to the complaints formulated both by the Commission and its European counterparts gathered together in the framework of Group 29, SWIFT has set up an *ad hoc* working group ("Data Protection Working Group") composed of officers of the financial institutions considered by SWIFT as representatives of its members and users. This working group has, among others, put forward modifications to be made to various existing contractual policies and the adoption of a new policy relating to the adherence to the Safe Harbor (see infra).

173. The deliberations of the *ad hoc* group were closed in July 2007. New documents governing SWIFT's contractual relationships with its clients (financial institutions) were then adopted by SWIFT's Board of Directors and published on 20 July (including on its website www.swift.com). The texts that were adopted modify, replace or complete the former terms and conditions and other contractual documents of SWIFT. This covers more specifically:

[73] The 2007 meetings with the secretariat of the Commission took place on 23 March, 13 April, 17 April, 24 May, 23 July and 16 August 2007.

- The *SWIFT Personal Data Protection Policy*, which distinguishes between the personal data collected for the management of its personnel or clientele, and the personal data collected by the clients of SWIFT that call upon the services of the company and processed in the framework of the provision of these services. In this document, SWIFT is qualified as a processor, in the meaning of the Privacy Act, as regards the processing of the data collected by the financial institutions and undertakes to comply only with obligations imposed on processors by Article 16 of the Privacy Act[74];
- The *SWIFT Data Retrieval Policy*, which describes **(1)** mainly the circumstances and conditions under which SWIFT may, to the benefit and at the request of the clients at stake, recuperate and return exclusively to such applicants the transfer data or the data contained in messages, when such data have been subject to a temporary back up by copy; the policy also describes the circumstances and conditions under which SWIFT would be likely to extract the backed up data in its possession **(2)** to aggregate them in the form of statistical results and then transmit such anonymous results to third parties (upon request of collective organizations in order to analyze and understand certain aspects of financial flows) or **(3)** possibly to respond to legally binding requests or injunctions rendered by a competent authority under the applicable law and transmit these data to the relevant authority;
- The *SWIFT Safe Harbor Policy* adopted in the framework of SWIFT's adherence to the Safe Harbor Principles that apply to European transfers of personal data to the United States and provides among others information on subsequent data transfers, on the security measures applied by SWIFT as well as on the procedure to be followed by the data subjects to access their data via the financial institutions.

- **The Adhesion to the "Safe Harbor Principles"**

174. On July 19, 2007, SWIFT declared its adherence to the safe harbor principles. SWIFT is since then mentioned in the public register of undertakings adhering to the Safe Harbor[75] in the "IT services" industry ("CSV"). A contractual policy relating to the safe harbor has thus been adopted (see supra). These measures were aimed at rendering the transfer and storage in the U.S. of personal data in the framework of SWIFT's commercial services compliant with Articles 21 and 22 of the Privacy Act.

[74] Irrespective of the processing that does not relate to the object of this recommendation and that is described by SWIFT under the category "personal data collected by SWIFT".

[75] See http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

- **The announced modification to the SWIFT's network architecture**

175. SWIFT's Board of Directors created a working group in charge of reviewing the various options for the revision of the SWIFT's network architecture. Further to the proposals of this working group, the Board of Directors has decided[76] in September 2007 to modify the network architecture and to create, by end 2009, a new operational center in Switzerland[77]. This reorganization of the architecture involves the regionalization of the operations carried out by SWIFT in the framework of its services, including the "back up" services ("Multiprocessing zones"). The objective is to process and archive the messages exchanged between SWIFT's clients pertaining to the European economic area, including Switzerland, in operational centers established in Europe, to the exclusion of the US-based center.

176. The network reorganization is motivated by considerations linked to data protection, but also by commercial strategies[78] aiming at canvassing and conquering new regional markets[79], and at improving the quality and performances of the services provided: resilience, security, cost reduction, etc.[80]

- **The information provided by SWIFT**

177. SWIFT has adopted measures aimed at ensuring information specific to the data processing that it carries out.

178. SWIFT's clients (the financial institutions) receive detailed information[81] on the implemented or likely to be implemented processing, through various policies, the online glossary ("Glossary"), the online Questions/Answers and personalized support if need be. SWIFT's new policies moreover indicate that client financial institutions must communicate to their own clients the information

---

[76] See SWIFT's press release of 4 October 2007 on www.swift.com.

[77] The European Commission has recognized that Switzerland offers an adequate level of protection to personal data which are transferred to it from the European Union. Moreover, Switzerland is party to Convention No. 108 of the Council of Europe *for the protection of individuals with regard to automatic processing of personal data* (see infra point 221).

[78] See interview of SWIFT's CEO, M. Lázaro Campos, Dialogue (The Voice of the SWIFT Community), Q2 2007: "*In some jurisdictions, our commercial appeal would be improved if we processed data in additional locations. We would attract more business to SWIFT. Data privacy would also be a factor to consider in this context*".

[79] The "SWIFT2010" objectives are attentive to the foreseen developments of the SEPA project ("Single European Payments Area").

[80] SWIFT's response of 16 November 2007 (point 3.1.iii) to the written questions of the Commission.

[81] Without prejudice to certain secured technical information.

relating to the processing of their personal data, carried out in the framework of the services provided by SWIFT[82].

179. SWIFT has also rendered a series of information on the processing carried out accessible to the general public, through its website: publication of the policies governing data processing; specific information regarding the injunctions of the UST; responses to the most frequently asked questions (including: location of operational centers, motive for the mirroring of the processing and the data, implemented security measures, etc.).

- **The absence of notification to the Commission and current situation as regards privacy**

180. In its opinion 37/2006, the Commission considered that SWIFT had the obligation to notify all the processing that it carried out, pursuant to Article 17 of the Privacy Act. As it considered that it was not the addressee of the opinion, as it contests the status of data controller and as, consequently, it does not consider itself bound by the obligations linked to such status, SWIFT had still not filed processing notifications with the Commission at the time of the opening of the present recommendation procedure.

181. In addition to its response to the conclusions of the rapporteur and the hearing of October 8, 2008, SWIFT submitted to the Commission two projects of notifications that correspond to the detailed analysis of the facts and the distinctions made by the rapporteur between those and the distinct responsibilities to which they lead: **(1)** in the capacity of *de facto* delegate of the community of its client users, for the processing for which this community is data controller, in accordance with the conclusions of the rapporteur and what is explained above (points 163 and 164), as well as **(2)** in the capacity of data controller of the processing with statistical and research purposes.

- **Measures aimed at preventing problems and guaranteeing effective exercising of the rights**

182. Moreover, SWIFT has adopted a series of measures and internal procedures aimed at verifying the observance of the Privacy Act obligations, preventing potential problems and guaranteeing that data subjects concerned by the processed personal data can, if the case may be, exercise effectively the rights granted to them by law.

---

[82] In that respect, Group 29 remains particularly attentive to the quality of the information provided by European banks to their clients.

183. A full-time Privacy Officer has been appointed within the company. In this capacity, he will be the preferred interface with the Commission.

184. A legitimate request coming from a data subject concerned by the processing of personal data will be handled by the services of the Privacy Officer. Since SWIFT is not in a position to reply directly to such requests given the absence of means allowing it to identify the relevant data contained in the messages (and given the fact that it should not have to bear the main cost of the obligations related to such requests – see below), it is provided that the company will invite the data subject to communicate the name of his/her bank and will transfer the request to the latter with a demand to respond to it and to inform it of the follow-up. This procedure is already expressly addressed in the Safe Harbor Policy (see above) but will be applied to the entirety of the legitimate requests, in particular those based on the application of the Privacy Act.

185. The Data Protection Working Group will be instituted on a permanent basis and will have as primary task to re-examine the SWIFT policies to assess the need to modify those in order to take into account the relevant elements of the present decision. In particular, this will involve determining to what extent it will be useful to specify internal procedures (notably the one described in the previous point) aiming to ensure the management of data subjects.

VI. THE APPLICATION OF THE LAW AND THE OBLIGATIONS OF THE DATA CONTROLLERS

186. The scope and content of the obligations which the company would be subject to or that it would have to bear must be determined whether SWIFT is acting as a *de facto* delegate of the community of its client users or in a marginal way as data controller,.

187. In any event, it must first be repeated that, for the processing for which they are data controller, the financial institutions are subject to the obligations set out in the law that applies to them.

V.1. THE FINANCIAL COMMUNITY

188. The financial community of SWIFT client users does not possess a precise and stable identity, nor an organization expressly constituted. Yet, for the application of the Privacy Act and according to its provisions, the data controller decides (the purposes and the means of the processing), but it must also be able to act, in particular to fulfill its legal obligations. The data controller must act and express itself in an identifiable manner for the data subjects, for the other data controllers with whom the data are exchanged, and of course for the control authorities such as the Commission.

189. It must be noticed that this community, with respect to the processing placed under its responsibility (see supra No. 163 and 164), acts through dialogue structures and procedures that it has chosen by creating the company and its functioning rules. SWIFT is in fact the organized catalyst of the community members' will, the place where the dialogue and the synthesis take place and, *in fine*, of the achievement and the expression of the collective will (see supra). Absent a different and distinct representation clearly identifiable, assumed and organized, and at least specifically with respect to the processing at stake and the application of the Privacy Act, SWIFT must be considered as the *de facto* delegate of the financial community of its client users (the latter being the controller of the relevant processing), representing this community from which it arises and to which it is bound by essence, and acting on its behalf[83].

[83] The designation retained (*de facto* delegate, "*délégué de fait*") corresponds the best to the situation such as established and described. The notion of "*de facto* representative" ("*représentant de fait*") would have created a confusion with the notion of "representative" within the meaning of the Privacy Act. *A priori*, the latter is not an operator intervening directly in the data processing, and for the situations which make its intervention necessary, it seems to have a personality more clearly

V.1.1. The obligations that favors or require a contact with the data subjects: quality of data, information, rights of access, rectification and opposition

- **In general**

190. SWIFT alleges that, if it were to be considered as data controller, it would be held to comply with obligations that would not apply to it as processor, that these obligations would require efforts that would be both disproportionate and useless (for instance if it were to perform verifications that have already been carried out) and that the large-scale operations to be conducted could turn out to be particularly dangerous for the security of the processing and the confidentiality of the data. This argument must of course be considered with as much attention as regards the same obligations placed under the responsibility of the financial community, if one were to consider that SWIFT – by delegation – had to comply with them.

191. Effectively, SWIFT does not exploit the identifying data of the data subjects (see supra) and does not possess the tools to access the processed data via the identifying data that it holds. Today, SWIFT could thus not perform an obligation that requires a direct contact with the data subjects (grant rights of access, rectification and opposition) or that requires at least an access to the identifying data (verify the quality of the data). Similarly, privileged information directly addressed to each data subject cannot be carried out by SWIFT. If the company were required to act in such a way, or if it decided to do so, it should develop a tool that would allow it to flag and manage these identifying data. This tool, the processing it would imply and the difficultly manageable exploitation possibilities that it would offer, could obviously harm the security of the processing currently carried out as well as the confidentiality of the data.

192. The rights of individuals should nonetheless be exercised, or the benefit that such rights guarantee should remain unaltered.

---

distinct from that of the data controller. The notion of "apparent data controller" ("*responsable apparent*"), on the basis of the appearance theory, could have implied a course of action which would exceed the authority and competences legally or contractually attributed, and an autonomy of decision-making for SWIFT, which does obviously not correspond to the way in which the company is really controlled and with which the decisions are effectively made. In fact, the appearance, in this case, would not engage the responsibility of the financial community on the basis of the actions of one of its members, bodies or agents which would have exceeded its authority or whose authority would have publicly taken the form of a consistent and admitted behavior. The appearance would result in separating SWIFT from the financial community, and result not in an apparent responsibility but in a real and autonomous responsibility (the data controller being only accountable to himself and for himself) which does not correspond to reality. The question is not only theoretical. The designation chosen, for what is underlying it and for what it enshrines, may have consequences on the effective application of the civil or criminal provisions, which does not fall within the Commission's competences. But, it may particularly, if it is not adequate, hide certain specific aspects of the organization of the identified community of interest and prevent one from drawing all necessary conclusions (see. infra, following numbers).

193. One may consider that, by default, SWIFT must bear and perform the obligations to which the financial community of its client users is bound in its capacity of data controller[84] and that, for that purpose and still by default, the relevant third parties may call upon SWIFT[85].

194. One must nonetheless assess whether SWIFT's delegation and the responsibilities that derive therefrom are not limited or contained by other delegations established or imposed by the facts, by the specificities of the connections and the commitments that bound SWIFT client users or also by the specific imperatives of the Privacy Act and its application.

195. In addition to the existence of a delegation on the part of SWIFT, established by default, in order to concretely determine the way according to which the obligations of the Privacy Act are or must be performed in the specific circumstance of a data controller constituted *de facto* by the gathering of multiple distinct entities, the facts that are specific to the situation may be reviewed in light of the following principles:

- the general principles governing mutual undertakings require that each of the members of a community (especially if it is voluntarily constituted in order to further a common interest) be naturally held by a duty of loyalty vis-à-vis the other members of the community;
- more specifically, the principle of good faith performance of mutual undertakings presumes among others that the members' legitimate expectations of the other members of the community be taken into account (and certainly those whose existence is clear) and an obvious cooperation according to which each bears the obligations that it is unmistakably the best suited or the only one suited to perform without undue burden;
- the application of the Privacy Act, as regards the determination of the responsibility of a data processing or of the burden of a specific obligation derived therefrom, is not limited or strictly held by the specific provisions of contractual law or commercial law; consequently, for instance, the protection of fundamental rights and liberties of individuals could not be upset or neutralized by the prevalence of rules that govern and organize contractual responsibility; the Privacy Act may thus admit the accountability of a burden, between the entities collectively constituting the data controller, to the entity that may best or that is the only one able to bear or perform the collective obligation without an undue effort, by possibly pushing aside certain

[84] Or at least to guarantee the performance thereof.

[85] As SWIFT carries out the data processing at stake in the Privacy Act by delegation of the financial community, nothing would allow considering that such delegation cannot be opposed to the data subjects, owner of the processed data.

rules that pertain to other areas of the law, when their strict enforcement would constitute an insurmountable obstacle to the protection of fundamental rights;

- unilateral undertakings, acts of acceptance or voluntary provisions on the part of the members of the community tend to reinforce, even to render unquestionable, the conclusions and decisions that may flow from the general principles governing mutual undertakings combined with the imperatives of protection of individuals' fundamental rights.

196. Concretely, several relevant elements may be underlined:

- financial institutions have (and are the only ones to have) direct contact with their clients and exploit the identifying data of the latter on a legitimate basis;
- the processing placed under the responsibility of the financial community, further to SWIFT's intervention, must necessarily and systematically be preceded by a processing placed under the responsibility of the payer's bank; they depend on it;
- the data processed under the responsibility of the financial community are necessarily and in any event identical[86] to those processed before, under the responsibility of the payer's bank;
- as responsible for the first processing and in that capacity, but also based on the rules and custom of the banking practice, of the fair performance of the mandate it is granted by its clients, of its responsibility towards the transaction's partners, or based on specific legal provisions[87], the payer's bank has to carry out the verifications required to ensure the quality of the processed data and the compliance with the conditions under which they may be processed (exactness, adequacy, relevancy, non-excessiveness, legality, no incompatibility of a later processing – all known – with the purposes of the collection, limited storage, ...);
- as responsible for the first processing, Belgian and European banks must inform the data subjects of the recipients of the collected and processed data; as the processing carried out by SWIFT (on any basis) is known and accepted [88] by banks, fairness, with which the latter must comply, require that they also inform their clients (being the "data subjects") of the processing purpose(s) that SWIFT will carry out (being the data "recipient");
- the processing placed under the responsibility of the financial community being the necessary consequence of the processing placed under the responsibility of the sending bank and relating to the same data, the rights of access, rectification and opposition could

[86] As it has been described, the nature and functioning of the system (and one of the purposes of the carried-out processing - see supra) imply and guarantee such perfect conformity.

[87] For instance, as regards combating money laundering and financing of terrorism (see supra).

[88] If not "determined" or "mastered", in the meaning of the Privacy Act, by the banks, processing is obviously known and accepted by them, including because it is subject to a contract with each of them, which describes and supervises it.

not be exercised vis-à-vis the financial community so as to produce a result other than if they were exercised towards the financial institution bound to respond in its role of data controller (and at least being the only one able to respond today)[89];

- generally, as regards the obligations of the Privacy Act requiring or favoring a contact with data subjects, financial institutions must, personally and vis-à-vis their clients, carry out activities whose content is identical or almost identical to those of the activities to be borne by the financial community for the processing for which the latter is responsible;
- financial institutions that use SWIFT messaging services are necessarily members of the SWIFT client users' community;
- financial institutions have, constantly and unanimously, regularly affirmed and confirmed that the company SWIFT was in their opinion the processor of each of them (including as regards the application of the Privacy Act with respect to all operations carried out by SWIFT) and that they should be considered as sole data controllers for the data contained in the orders of their clients; this affirmation (which is only a point of view) does not by itself establish the legal status and status of SWIFT, but it allows one to consider that banks, by presenting themselves as data controllers, were ready to carry out the legal obligations linked to such status (including for the processing that a review of the facts leads to place under the responsibility of the financial community) and did commit to doing so.

197. The elements presented here, assessed in light of the principles allowing for a possible allocation of the charges linked to the obligations of a data controller, naturally lead one to attribute to each of financial institutions members of the SWIFT client users community the responsibility to carry out the obligations to which the community is held, whose content is similar to the obligations to be otherwise individually performed by each of them for the processing placed under their personal responsibility. Moreover, these obligations may currently only be materially assumed by the financial institutions, and their content is strictly and exclusively limited to what concerns their own clientele.

198. The delegation by default, which was made by the community of its client users to the benefit of SWIFT, and the requirements that may be derived therefrom as regards the obligations imposed by the Privacy Act, must therefore be appreciated, contained and limited by the charges attributable to each financial institution member of the community, that all obviously agree to carry out.

---

[89] The institutions located on the territory of the European Union are obviously held by the provisions of Directive 95/46 and the implementing national legislations; but contractual or custom-based provisions that govern banking practice and fair relationships with clients may more largely produce the same effect.

199. As regards specifically the follow-up to be given to binding injunctions of administrative or judicial authorities, and without this presupposing anything regarding the qualification which will always have to be assessed case by case (see supra), the existence of what could be considered as an explicit *de facto* delegation from the community to SWIFT (in the case where its community of client users would have to be designated as data controller for certain processing) should, however, be considered as established by the "Data Retrieval Policy" and the exercise of which would therefore be strictly regulated by the latter.

- **Specifically as regards the obligation to inform**

200. The controller whose processing is subject to the Belgian and European legislations must provide data subjects with a series of information in relation to the processing that their personal data do, will or may potentially[90] undergo. This information must not be provided again or even on another basis "if the data subject is already informed thereof", whether the data controller has obtained the data from the latter or from another source[91]. The information that must personally and mandatorily be offered by the banks is likely to offer such prior knowledge.

201. The making available to the public by SWIFT of information on the processing carried out by the company (see supra) moreover participates in the general performance of the information obligation. This public information is likely to offset a possible imperfection of the information provided by the banks, in particular the banks that are not located on the territory of the European Union.

202. Moreover, taking into account what has been or should be accomplished by the banks, one must remember that the data controller is relieved from providing the information mentioned in the law (or a part of this information if another could be provided) "when (…) the information of the data subject appears impossible or implies disproportionate efforts"[92]. The impossibility or the disproportion of the efforts to be devoted must of course be justified and reasonably motivated (including in the processing notification to be filed with the Commission). In that respect, "may be taken into account the number of data subjects as well as the compensating measures that may be [that have been] adopted"[93]. The above elements refer to such measures.

---

[90] This should of course relate to a foreseeable possibility, supposed to occur when known conditions are fulfilled.

[91] Article 9, § 1, al.1 and § 2, al. 1 of the Privacy Act.

[92] Article 9, § 2, al. 2, litt. a and b.

[93] Directive 95/46/CE, Recital 40.

203. Moreover, certain information should not be provided (by SWIFT, if it were held that only the company would be in charge of the information on behalf of the financial community) “to the extent that, considering the specific circumstances under which the data are processed, this information is not necessary to ensure a fair processing of the data as regards the data subject"[94]. Considering the general information that is ensured and the fact that SWIFT does not exploit the identifying data contained in the messages, and does not possess at this moment a tool that would permit doing so, the circumstances would clearly be met for the processing at stake.

- **Specifically as regards the rights of access, rectification and opposition**

204. If, by hypothesis, one should suppose that the specific charges of the financial community regarding the access, rectification and opposition could not be attributed to each of the members of the community as regards its own clientele, or if some people would contest such attribution, one could nonetheless not ignore the obligations that already and otherwise exist on the part of each financial institution with respect to its clients, pursuant to the right that applies to it and pursuant to the general rules of the banking practice. An access, rectification and opposition request directly sent to SWIFT and that would require that SWIFT respond to it by itself, would be clearly devoid of interest[95], clearly disproportionate[96], and thus abusive.

205. It is useful to repeat that the opposition right may in any event not be exercised[97] when the processing is required by the performance of contract to which the data subject is a party"[98] or when it is “necessary to the compliance with a legal obligation that applies to the data controller"[99].

206. Moreover, with SWIFT intervening to certify the integrity of the data transferred by the issuing bank and communicated to the recipient bank, one may hardly imagine that the company would intervene to rectify the data without referring to these two actors. Even considering that SWIFT may have access to the identifying data of the applicants, the rectifications that,

---

[94] Article 9, § 2, al. 1 in fine.

[95] The information being known or being easily obtained or corrected at other sources.

[96] Obvious disproportion between the lack of interest, the effort to be exerted by SWIFT to respond to the request for which it does not currently possess the necessary tools and the risk that the result of such effort would constitute (the production of such tools and the additional data processing carried out or rendered possible).

[97] Article 12, § 1er, al. 2 of the Privacy Act.

[98] Article 5, al. 1er, b.: the contract with the bank and the order given to the latter in the framework of the contract, provided of course that each party (and most of all, the client of the bank) is duly informed of the conditions and implications of the contract.

[99] Article 5, al. 1er, c.: the binding (and legal) injunction of an authority constitutes such an obligation; in most countries today, banks are for instance required to report suspect orders on the basis of the criteria that are provided to them by the authorities (combating money laundering and financing of terrorism etc.).

hypothetically, the company would carry out should necessarily be passed on to the institutional partners to the transaction (perhaps regardless of the binding legislations that require them to store, for longer than SWIFT stores them, data linked to a transfer order, that they have the means to verify and that they would have all reasons to consider as correct). It is indeed at the level of the issuing bank that the right of rectification must be exercised (to the extent that it may be exercised), the right exercised at the level of SWIFT (theoretically envisaged) being without object without prejudice to the lack of interest that one would have to exercise it. Moreover, rectifications could, hypothetically, be brought by SWIFT only to data of messages temporarily archived in the processing centers of the company: they would thus only relate to financial transactions already executed. In that sense, as they reflect these transactions and the elements of information that have surrounded their execution, one must consider that the data at stake are necessarily correct.

V.1.2. Publicity (the notification of the processing)

207. Acting by delegation of the community of its client users, SWIFT must bear and perform the obligation to notify the Commission, pursuant to Article 17 of the Privacy Act, of the treatment that the company carries out and which is placed under the community's responsibility.

208. Nothing identifies a delegation for which another person would have been specifically entrusted in order to perform this task. It is then on the basis of its delegation by default that SWIFT must act.

209. The processing carried out by delegation and placed under the responsibility of the financial community could be subject to one notification, grouped under the generic purpose: "to contribute to the safety of financial transactions through the automated and secured transmission of standardized, integer and immediately exploitable information" (possibly detailed and explained by the indication of specific purposes that are different but linked to one another – see supra). The transfer, the mirroring and archiving in the United States should not be subject to a separate notification, to the extent that this processing is not conducted for different purposes. The transfer to the United States should nonetheless be subject to a specific reference, pursuant to the law. The uselessness or the impossibility to directly inform the data subjects should also be motivated.

210. There is no legal objection against the fact that the notification would explicitly mention the delegation through which SWIFT intervenes and would identify the actual responsibility of the financial community of the SWIFT client users (community in fact tacitly but effectively constituted by a constant and collective practice as regards the services performed by SWIFT). Such an indication is moreover advisable in order to specify the way according to which the rights of access,

rectification and opposition should be exercised. The clarity vis-à-vis data subjects moreover guarantees their ability to act in accordance with their best interests in case of civil damage.

V.1.3. Enforcement of the law as regards transfers outside the European Union

211. The transfers of personal data carried out by SWIFT to a country not a member of the European Union are placed under the responsibility of the SWIFT client users' community. They deal exclusively with real-time duplication of the processing and the archiving performed in the United States on the basis of the messages initially received in the processing center in the Netherlands.

212. As long as no express and relevant rules exist in this regard between members of the SWIFT community of client users, the burden of the obligations relating to this responsibility should be executed by SWIFT in its capacity as *de facto* delegate of the data controller.

213. Article 21 of the Privacy Act requires that "the transfer of personal data subject to a processing after their transfer to a country not a member of the European [Union] may only take place if such country ensures an adequate level of protection and subject to the compliance of other provisions of this act". In the absence of any other indication and as long as it is not established by a competent authority in an enforceable decision that the level of protection of the concerned country is either adequate or insufficient, it is the data controller (of the transfer) that must ensure this provision is indeed being applied, taking into consideration all the relevant factual and legal elements.

214. By its Decision 2000/520/EC of July 26, 2000, the European Commission has established that "for all the activities falling within the scope of Directive 95/46/EC, the "Safe Harbor Privacy Principles" (...) are considered to ensure an adequate level of protection for personal data transferred from the community to organizations established in the United States" provided that "the organization receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs[100]" complies with the other provisions of the Decision and of its six annexes.

215. Article 25, §6 of Directive 95/46/EC requires that "Member States shall take the measures necessary to comply with the [European] Commission's decision".

---

[100] Article 1, §§1 and 2 of Decision 2000/520/EC of the Commission pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce.

216. As an organization with a fixed establishment in the U.S., recipient of personal data transferred from the European Union, SWIFT declared its adherence to the safe harbor principles on July 19, 2007.

217. Generally, it cannot be disputed that, since then, the transfers of data to the United States have complied with the requirements of the Privacy Act and that SWIFT no longer has to justify the adequate protection the transferred data should benefit of, and [that SWIFT does not have to] evaluate the legality of the transfer.

218. One must, however, keep in mind that Decision 2000/520/EC only covers in a mandatory and undisputable fashion "the activities falling within the scope of Directive 95/46/EC". Police and judicial matters are clearly excluded from the scope of the directive (Dir. 95/46/EC Article 3.2). Moreover, the European Court of Justice has made clear that the directive regarding data protection (and the possibilities it instates) does not apply to processing of data first collected by private persons that are subsequently accessed for purposes of public safety[101].

219. Annex IV to Decision 200/520/EC, constituting one of the explanatory documents produced by the U.S. Department of Commerce, also provides: "The safe harbor principles contain an exception where statute, regulation or case-law create conflicting obligations or explicit authorizations (...). Clearly, where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law. (...) Where the law specifically authorizes the company to provide personal information to government agencies without the individual's consent, this would constitute an explicit authorization to act in a manner that conflicts with the safe harbor principles".

220. It clearly appears from the above that the communications of messages (and of data) to the UST, in execution of binding injunctions addressed to SWIFT by such administration, are not covered by the authority of Decision 2000/520/EC of the Commission and do not benefit on that basis of the objective and prima facie reputation of adequate protection.

221. Yet the Privacy Act, contrary to Directive 95/46/EC, governs also the processing of personal data carried out in a police or judicial framework and extends to those processing the scope of the protection guaranteed to the data subjects and the requirement of an adequate protection of

---

[101] ECJ, "PNR" judgment, joined cases C-317/04 and C-318/04, 30 May 2006. Also read on this P. DE HERT and R. BELLANOVA, Data protection from a transatlantic perspective: the EU and the U.S. move towards an international data protection agreement?, study requested by the Commission for Civil Liberties, Justice and Home Affairs, Publications of the European Parliament (EP 408.320), October 2008.

the transferred and subsequently processed data for purposes of public safety. In the present case, Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data also applies. Convention No. 108 also requires of an adequate protection of transferred data, including when they are likely to be processed for purposes of public safety. The requirements in terms of protection demanded by Convention No. 108 are, however, much less precise and strict than those provided by Directive 95/46/EC. Nevertheless, it remains that, absent an objective and enforceable decision from a competent authority, the data controller (the controller of the file under Convention No. 108) must be able to provide guarantees that the data it transfers will benefit from adequate protection on the occasion of a possible subsequent processing for purposes of public safety by a competent authority of the receiving country.

222. On the basis of Article 24 and 38 of the Treaty on European Union, the European Commission and the Council of the European Union are competent to conclude international agreements, notably in judicial and police matters. As regards the communications of messages and data to the UST within the known limits of the injunctions addressed on the basis of the fight against terrorism financing, the UST Representations together with the responses of the European Commission and of the Council of the European Union, published on July 20, 2007 (see supra) and the authority that is attached to these documents, have lifted the potential uncertainty as regards the adequate protection (in the light of the legal requirements) of the data transferred to the United States and have filled the obvious limits of the objectively recognized protection that is guaranteed by the adherence to the safe harbor principles. It is important to underline that the Representations of the UST expressly aimed at establishing the respect of the protection rules contained in Directive 95/46/EC. Even though the latter may not be applicable, it is effectively the high level of protection that it provides which has been used as the reference for the unilateral undertaking of the UST to the agreement between the U.S. and EU authorities.

223. One may not legally dispute that, by the authority of the decisions of the European Commission, the requirements of the European provisions and of those of the Privacy Act are indeed met; that, within the limit of all situations having taken place or that may be foreseen, known and described, the transfer of personal data from the Netherlands to the SWIFT processing center located in the United States is thus in perfect compliance with the law; and that, as a consequence, the processing subsequent to the transfer, carried out specifically on the basis of data physically archived in the U.S. center, escape the Commission's assessment regarding the quality of the transfer[102] and this for as long as the provisions of the decisions of European authorities are strictly

[102] This is certainly true in the context of a procedure aiming to control compliance with the law and which could lead to issuing recommendations to a data controller. The assessment of the Commission remains more free in the context of an

complied with. In any case, even though the rules of a third country to the European Union can be assessed to evaluate the quality (and hence the legality) of a data transfer (and possibly to forbid such on the ground of an insufficient protection), the Privacy Act is not and shall obviously never be applicable on the territory of this third country as regards the processing of personal data which are physically located there.

VI.2. THE SWIFT COMPANY

224. For processing conducted occasionally, depending on the specific circumstances, and for which SWIFT is directly responsible, one must also assess the scope of the legal obligations to be borne by the data controller and that the company could be required to comply with in order to carry it out.

225. One must underline that the processing placed under SWIFT's responsibility is, will and may necessarily only be carried out on data contained in a temporary general base (archiving), whose creation and maintenance are placed under the responsibility of the financial community.

226. As already mentioned, the obligations linked to the quality of the data have already been complied with.

227. The processing for statistical purposes does not present incompatibilities with the initial purposes of the collection, when it is carried out under the conditions set forth by the King in accordance with the law. As SWIFT carries out the anonymization of the exploited data by isolating them from the identifying data before their statistical processing, such conditions are clearly met.

228. Similarly, the exercise of the rights of access, rectification and opposition cannot be considered in the event of anonymous data.

229. The processing carried out marginally under SWIFT's direct responsibility for statistical purposes should nonetheless be subject to a notification of specific processing, be it to ensure a perfect transparency with respect to the anonymization process and the exploitation of anonymous information.

---

advice procedure, which could bring the Commission to give its opinion on possible deficiencies of the law and the need to amend it.

VII. CONCLUSIONS

VII.1. THE NEED TO ASSESS FACTS IN CONTEXT

- **As regards the treatment carried out in the framework of the services provided by SWIFT**

230. SWIFT has considered itself as a processor for all data processing carried out by the company in the framework of its commercial activities. The company has therefore not fulfilled the obligations imposed by law upon data controllers, including by not filing any processing notification with the Commission (and, thereby, by not notifying the transfer and archiving in the United States). SWIFT has maintained this position after the opinions rendered in 2006 by the Commission and Group 29. This reminder must, however, also be put into context. Since about 35 years, SWIFT disposes of an exploitation unit in the United States, to which the data it processes are transferred and where these data are temporarily archived without this being unknown. At no time, since the entry into force of the Privacy Act more than 15 years ago and until June 2006, did SWIFT's activities and the data processing conducted in that framework lead to preoccupations, interrogations or a specific attention with respect to the rules and obligations of the successive legislations governing personal data processing. The Commission was never seized of any complaint or of information justifying an investigation. Generally, no authority was concerned with the situation, has suspected possible infringements of the Privacy Act nor has showed any fear as regards a potential risk. The absence of collective attention does not constitute, of course, an excuse for behaviors that are contrary to the law. But it must strongly adjust the severity of judgments and appreciations, especially if no decisive element allows one to contest, in this general context, SWIFT's good faith and the absence of fraudulent or deceitful intention. It must be underlined that SWIFT's exploitation unit was established in the United States 25 years before the new provisions relating to data transfers to States that are not members of the European Union entered into force in Belgium (in 1998). One may not easily reproach SWIFT for the absence of reorganization of its network at that time, as no problem appeared to exist.

231. One must also underline that, as of the Commission's first opinion in 2006, SWIFT has presented its position through argued notes and written submissions. One may thus not hold against SWIFT its passivity with respect to the decisions that it contested. These exchanges have continued until the current procedure and have probably led SWIFT, among others, to decide on measures that have since been adopted by the company, and which have been mentioned.

- **As regards the data transfer to the UST**

232. It does not appear questionable that SWIFT was compelled to abide by the UST's injunctions and could not materially avoid them, including because one of its two processing and archiving centers (and the information that are physically kept therein) is located on the territory of the United States. At least, it cannot be questioned that SWIFT's Board of Directors has reached this conclusions after having raised objections and obtained guarantees regarding the exploitation of the transferred data. The situation would have obviously been different if, by invoking the extraterritorial effects that the U.S. legislator had meant to give to the applicable legal provisions, the UST had ordered SWIFT to communicate data physically held outside the U.S. territory. It is not relevant here to regret that SWIFT has not undertaken certain steps, or to indicate that it would have been required to take such steps pursuant to the Belgian and European legislations to which it remains bound (including steps informing Belgian and European data protection authorities). These considerations would be even less grounded today as the intervention of the U.S. authorities with respect to SWIFT was (even in a limited way) already known in 2002 and exploited in the framework of international actions against terrorism financing. Informative steps towards European data protection authorities would have perhaps been likely to differently frame the responses given to the U.S. injunctions. In any event, pending a possible regulatory framework established and shared by U.S. and European authorities, which SWIFT did not have the task to negotiate, these steps, how important they may have been, would have not altered the binding force of the UST injunctions. One must also understand that in the balance of risks that SWIFT's Board of Directors has realized, it has considered that it would obtain greater guarantees and a greater protection of the transferred personal data in a discussed framework[103], whereas an attitude of radical opposition would have offered none, and would have certainly lead the U.S. authorities (possibly confirmed by a court) to carry out a data seizure even larger than the batches that were effectively transferred and whose exploitation was controlled by scrutinizers designated by SWIFT and today by the "eminent European person". The large dissemination by the U.S. press of facts that have drawn attention to SWIFT has certainly liberated the company of a heavy burden. But no one can predict what would have been SWIFT's behavior over time in the absence of such revelation, and blame SWIFT on that basis.

233. Generally speaking, it appears therefore difficult to draw arguments from past facts that would justify proceedings, or any sentence, against SWIFT.

---

[103] By the debated challenge of the likely disproportion of the first injunctions and their legality, up to consider, due to the guarantees obtained, to no longer have any argument to raise before a jurisdiction, enabling one to establish the excessive scope of the subsequent injunctions.

234. Moreover, it should briefly be repeated, as additional assessment elements, the quality of the processing carried out by SWIFT and the procedures and protections that apply to them, that securitize them and that prevent risk of damaging processing or illegitimate exploitations of the data, as these procedures and protections have been established and described here.

VII.2. THE NEED TO DRAW USEFUL LESSONS

235. One must nonetheless admit that the risk of an exploitation of the data transferred by SWIFT to the United States that would ensure to the latter adequate protection is not completely put aside although it remains theoretical.

236. Other binding administrative injunctions could be addressed to SWIFT, as to any organization established in the United States, pursuing other objectives than the fight against terrorism financing. The current decisions would not guarantee, a priori and authoritatively, the existence of an adequate protection of the data so obtained.

237. Be it SWIFT[104] or a data controller placed before the same legal obligations (in the United States) and the same uncertainties (as regards compliance with European legislations on protection of personal data), it would be expedient for the European authorities to continue maintaining specific attention as regards the question, and for them to succeed in formally instituting a mechanism able to receive the description of the issue, to guarantee the confidentiality of the information and to officially support the dialogue and the negotiations perhaps necessary with the U.S. authorities in order to establish adequate protection rules, governing the subsequent exploitation of requested or seized data.

238. Today, one could not reasonably require entities confronted with similar situations to report only and simply, without further assurance, to the controlling authority of the country of origin of the data or even to the assembly of European controlling authorities (G29), facts for which U.S. law imposes secrecy and whose disclosure is criminally sanctioned, and for which, in case an obvious lack of protection would be established, even temporary, these authorities could not legally ensure the confidentiality. But these authorities should of course be associated to the mechanism of regulation and guidance briefly described.

---

104 Executing as *de facto* delegate the obligations of the data controller.

239. In the absence of such a solution, the data controller of the processing constituted by the transfer of data outside the territory of the European Union will remain bound to guarantee the adequate protection of the data actually transferred and, as the case may be, to obtain assurances and supervising measures organizing a specific protection, almost custom-built.

240. The attitude adopted by SWIFT since 2001 when faced with the injunctions that it received from the UST was severely criticized in 2006, directly after the dissemination of the information published by the *New York Times*. The company was accused of having adopted a light, even self-indulgent, attitude and having blatantly violated Belgian and European legislations on personal data protection. These facts must be assessed today on the basis of better knowledge and in light of the subsequent events and developments, and one must draw, as an example, the lessons useful for those who, tomorrow, would have to take on the obligations of data controller required, under legal pressure, to communicate important files to an administration of the United States (or, in an equivalent context, of another State that is not a member of the European Union).

241. It is difficult to discredit the supervising measures granted since 2002 by the UST to SWIFT in response to the objections of the Company, if one considers the Representations and the unilateral undertakings addressed by the same U.S. administration to the authorities of the European Union and accepted by the latter, confirming and maintaining unaltered all guarantees granted to SWIFT and the functioning of the investigation system, subject to further details as regards durations of the storage of copies of the obtained messages and to the role attributed to the independent “eminent European person” to control all processes and their compliance with the established framework. Moreover, if one must be happy with the existence of control mandated by a public authority, the powers of control, audit and intervention granted to the “eminent European person” are the same as those offered to the independent scrutinizers acting on behalf of SWIFT.

242. With small differences (and within the limit which the status of SWIFT – private company – could allow it to obtain), the measures for which the European authorities have considered that they guaranteed an adequate protection of the data first transferred to the United States and then requested by the UST, are the same than those which SWIFT has benefited from.

243. Taking into account unquestionable elements of international legality that could be invoked[105] and the existence of information on the facts brought to the knowledge of certain , even limited, in support of official recommendations to the other States to act likewise (see supra n°16),

---

[105] Although they may of course be criticized, be subject to legitimate challenges and constitute a basis for claims in favor of contrary decisions, these legal elements do exist and SWIFT should not have to bear the criticisms that are leveled at them.

also taking into account the nature and the scope of the guarantees granted to SWIFT in this consensual context and of the subsequent acceptance of the adequacy of these guarantees by the European authorities, it would be contradictory and incorrect to allege today that the communications of data carried out by SWIFT in execution of the binding injunctions that it received from the UST did not benefit, as regards our legislation and its requirements, from an adequate protection even before the agreements between the European and U.S. authorities.

244. It is SWIFT who guaranteed the existence of an efficient protective framework. The latter could always have been broader. Moreover, nothing indicates that SWIFT could not obtain more guarantees by adopting another attitude. But nothing points to the contrary either. SWIFT's attitude was perhaps not the only adequate one (although it would be highly questionable to defend, outside any context, other choices supposed to be better and obvious), but one may say, in any event, that it adopted a prudent, diligent and attentive conduct, amid the stakes involved, to the protection of personal data transferred from the European Union. One may moreover underline that the guarantees granted for the European data have also benefited, at SWIFT's request, personal data with a U.S. origin, because they were initially received in the processing center located in the United States (see supra).

245. Even if one may under no circumstances institute it as an unquestionable model of conduct to be adopted in similar situations, SWIFT's attitude may in any event be used as a reference. Even more, the guarantees and protection that have been granted to the company (and the demonstrated existence of an international legality accepted by most of the States) may serve as reference and as assessment tool to take position and to found the objections that could be opposed to more significant injunctions and requests, devoid of the same framework and perhaps – in that sense – disproportionate.

246. The burden of this responsibility, left to the data controller of the personal data processing only, obviously pleads in favor of the quick creation and putting in place of the European assistance mechanisms already suggested above. The institution of a high-level EU-U.S. Contact Group on the protection of personal data as of November 2006 is a step in this direction. In the context of the new relations and exchanges between the European and U.S. authorities, one could consider from now on that situations similar to the one SWIFT has experienced should in any case, whatever the guarantees obtained directly from the requesting authority, be brought to the knowledge of the Contact Group by the concerned data controller (or by the spontaneously informed control authority). This cautious attitude (which does not excuse one from putting in place alternate means to guarantee adequate protection) could not be subject to blame by the U.S. authorities given that they have precisely committed to having problematic situations examined by the Contact Group. This

attitude would demonstrate a loyal and effective exercising by the data controller of the obligations that are its own while assuring itself of support in dealing with the difficulties with which it could be confronted.

ON THESE GROUNDS,

- **As regards the present recommendation procedure**

247. Recording that SWIFT has notified to the Commission: **(1)** the processing that it carries out as *de facto* delegate by default of the community of its client users and **(2)** the processing subject to the provisions of the Privacy Act that it marginally carries out as data controller, the Commission:

- acknowledges that at this day, SWIFT, acting by delegation of the community of its client users for the processing for which the latter is data controller or acting marginally as data controller, complies with all provisions of the Privacy Act;
- decides that there is obviously no need for a recommendation;
- hereby closes the present procedure.

- **As regards the initiatives undertaken by SWIFT**

248. In addition, the Commission officially notes the own initiatives undertaken by SWIFT or by the financial community through SWIFT that are likely to reinforce and that are directly aimed at reinforcing the protection of fundamental rights and liberties of individuals in the course of the processing of their personal data carried out in the framework of the services provided by SWIFT, favorably assesses these initiatives and encourages them:

- the decision to install a new processing center in Switzerland to ensure the mirroring of the processing and of the temporary archiving of messages sent between financial institutions from the European territory;
- the appointment of a full-time Privacy Officer within the company;
- the formalization of procedures managing the exercise of their right by data subjects who contact SWIFT;
- the evaluation of the policies which bind SWIFT to its users and clients and which structure the community of interests that the latter constitute.

249. The Commission requests to be informed of the follow-up given to these initiatives.

- **As regards the perspectives for the financial community**

250. The Commission draws the attention of the financial institutions members of the community of SWIFT client users that are located on the territory of the European Union, with respect to the interest of establishing collectively common rules to ensure the information to be communicated to their clients and to guarantee the efficient exercise (when it is justified) of the rights of access, rectification and opposition regarding the data processing carried out in the framework of the use of the SWIFT's messaging services and placed under different successive responsibilities, it being understood: **(1)** that each financial institution must of course remain in charge of the proper application of these rules toward its clients; **(2)** that the development of these rules should be subject to an accompaniment by Group 29 (on the basis of the advice the latter has already issued) in order to guarantee the same assessment in all Member States of the European Union.

251. The Commission asks SWIFT to inform the financial community of its client users of the content of the present decision.

- **As regards the useful lesson that can be drawn**

252. Pursuant to Article 14 of the IR, the Commission decides to notify officially the European Commission and the Group 29 of the present decision, drawing their attention on points 235 to 246, and wishing that they remain entrusted in an effective way with the questions raised therein.

For the Administrator i.c., The President,

(sig.) Patrick Van Wouwe (sig.) Willem Debeuckelaere