



06/EN

**Press Release on the SWIFT Case
following the adoption of the Article 29 Working Party opinion on the processing of
personal data by the Society for Worldwide Interbank Financial Telecommunication
(SWIFT)**

23 November 2006

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

At its last session on November 21/22, 2006 the Article 29 Working Party has again been dealing with the SWIFT case and has unanimously adopted Opinion 10/2006 (WP 128) on its findings in this case.

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

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

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

CONCLUSIONS:

In its opinion no 128 dated November 22, 2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) adopted today, the Article 29 Working Party comes to the following conclusions:

- a) The EU Data Protection Directive 95/46/EC is applicable to the exchange of personal data via the SWIFTNet FIN service;
- b) SWIFT and the financial institutions bear joint responsibility in light of the Directive for the processing of personal data via the SWIFTNet FIN service, with SWIFT bearing primary responsibility and financial institutions bearing some responsibility for the processing of their clients' personal data.
- c) SWIFT and the financial institutions in the EU have failed to respect the provisions of the Directive:
 - (i) *SWIFT*: As far as the processing and mirroring of personal data in the framework of the SWIFTNet FIN service is concerned, SWIFT as a data controller must comply with its obligations under the Directive, amongst which, the duty to provide information, the notification of the processing, the obligation to provide an appropriate level of protection to meet the requirements for international transfers of personal data;
 - (ii) *Financial institutions*: The financial institutions in the EU as data controllers have the legal obligation to make sure that SWIFT fully complies with the law, in particular data protection law, in order to ensure protection of their clients. The financial institutions are responsible for having sufficient knowledge of the different payment systems and their technical and legal characteristics and risks. If financial institutions did not strive (sufficiently) to obtain such knowledge, they would accept

substantial legal and client risks in breach of their fundamental duty of care. In particular, if some services such as the SWIFTNet FIN service involve massive transfers to countries without adequate data protection in the light of the Directive or if it is likely that such transfers would pose specific privacy concerns or risks, the Working Party is of the opinion that it is essential that the individual clients of the financial institutions are informed by the financial institutions, as their providers of professional services, in accordance with the transparency requirements of the Directive.

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

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

- e) The Working Party recalls once again¹ the commitment of democratic societies to ensure respect for the fundamental rights and freedoms of the individual. The individual's right to protection of personal data forms part of these fundamental rights and freedoms. The Community Directives on the protection of personal data (Directives 95/46/EC and 2002/58/EC) form part of this commitment. These Directives aim to ensure respect for fundamental rights and freedoms, in particular, the right to privacy with regard to the processing of personal data and to contribute to the respect of the rights protected by Article 8 of the European Convention on Human Rights, and Article 8 of the EU Charter of Fundamental Rights. In all these instruments, exceptions to combat crime are provided for but have to respect specific conditions.

IMMEDIATE ACTIONS TO BE TAKEN TO IMPROVE THE CURRENT SITUATION:

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

- a) **Cessation of infringements:** SWIFT and the financial institutions shall comply with their legal obligations under national and European law. This includes taking steps to ensure that any transfers of personal data are in line with the law. In the case of non-

¹ Article 29 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism; WP 53, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm .

compliance, data controllers can expect to be subject to sanctions imposed by the competent authorities under the Directive and national law, in order to enforce compliance.

- b) **Return to lawful data processing:** The Article 29 Working Party calls upon SWIFT and the financial institutions to immediately take measures in order to remedy the currently illegal state of affairs, and to return to a situation where international money transfers may be made fully in compliance with the data protection law. The Working Party welcomes that some DPAs are already today urging the financial institutions to find a solution without delay.
- c) **Actions as regards to SWIFT:** For all its data processing activities, SWIFT as a controller must take the necessary measures to comply with its obligations under Belgian data protection law implementing the Directive.
- d) **Actions as regards to Central Banks:** The present situation calls for a clarification of the oversight on SWIFT. The Working Party recommends that appropriate solutions are found in order to bring compliance in particular with data protection rules clearly within the scope of the oversight, without prejudice to the powers of national data protection supervisory authorities, as well as to ensure that relevant authorities are duly and timely informed where necessary. The Working Party considers that the lack of compliance with data protection legislation may actually hamper consumers trust in their banks and might thus affect also the financial stability of the payment system (reputation risk). Legal obstacles such as professional secrecy obligations of the overseers that could be used as argument to limit the effective control by the independent data protection authorities, shall not be relied upon in case of possible violation of constitutional or human rights.
- e) **Actions as regards to Financial institutions:** All financial institutions in the EU using SWIFTNet Fin service including the Central banks have to make sure according to Articles 10 and 11 of the EU Directive 95/46/EC that their clients are properly informed about how their personal data are processed and which rights the data subjects have. They also have to give information about the fact that US authorities might have access to such data. Data protection supervisory authorities will enforce these requirements in order to guarantee that they are met by the all financial institutions on a European level and they will cooperate on harmonized information notices. The Article 29 Working Party recalls in this connection its opinion adopted on harmonized information provisions². It also seems appropriate for financial institutions and Central Banks to consider alternative technical solutions to the procedures that are currently used, in accordance with the principles of the Directive.

The Working Party also stresses the following:

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

² Article 29 Working Party “Opinion on More Harmonised Information Provisions”, 25 November 2004. WP 100; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

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

Opinion 10/2006 (WP 128) will soon be published on website http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm in the various languages of the European Union.

Done at Brussels, on 23 November 2006

For the Working Party
The Chairman
Peter Schar