úřad pro ochranu osobních údajů
the office for personal data protection

Press Release on SWIFT case

In June 2006, Privacy International informed the Office for Personal Data Protection, as well as other similar supervisory authorities in the area of personal data protection in the EU Member States and in other countries, that the SWIFT company had been providing data on international financial transactions to the U.S. authorities in the framework of the fight against terrorism, without knowledge of the clients of the financial institutions.

Privacy International is a private organization founded in 1990 with its seat in London, comprising members from 30 countries; its objective is to safeguard privacy, human rights and civic freedoms.
SWIFT (Society for Worldwide Interbank Financial Telecommunications) is a global financial service which facilitates international money transfers. It is a company with co-operative characteristics, established and operated under Belgian laws, with its headquarters at the seat of the National Bank of Belgium. It has a number of offices in various countries (none in the Czech Republic). An important role in the supervisory bodies of the company is played by the central banks of the G-10 countries which have delegated their basic control powers to the National Bank of Belgium.
The information provided by Privacy International and the results of the subsequent investigation carried out particularly by Belgian authorities further indicate that SWIFT has two centers of operations, one in the EU and the other in the U.S. The U.S. branch acts as a "back-up" and precisely mirrors all relevant operations. On the basis of an agreement concluded between SWIFT and the U.S. authorities, large quantities of data are transferred from the operations center to "black boxes" that are under the control of the U.S., probably on the basis of approximate specifications, such as "from-to", "country-country", "bank-bank", etc.; the U.S. Department of Treasury then collects individualized data from the black boxes. All the above takes place on the basis of official requests for information ("subpoenas") that are binding for entities operating within the jurisdiction of the U.S.

The issue of provision of personal data by the SWIFT company to the U.S. authorities within the fight against terrorism has also been dealt with by the Article 29 Data Protection Working Group ("WP 29"), which is an independent advisory body of the European Commission consisting of the heads of the national supervisory bodies for the area of personal data protection.
On November 22, 2006, WP 29 adopted a detailed opinion on this matter (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_cs.pdf). In the opinion, it noted violation of several provisions of the relevant Directive concerning personal data protection (95/46/EC) and, consequently, also the corresponding provisions of the national regulations. This includes particularly the fact that large quantities of data had been provided for a purpose that its incompatible with the original commercial purpose of their collection (Art. 6 (1) (b) of the Directive). Neither SWIFT nor the financial institutions informed the data subjects of the manner of processing their data in relation to their transfer to the U.S., as required by Art. 10 and 11 of the Directive. Art. 25 and 26 of the Directive, which stipulate the conditions for a transfer of data to "third" countries with inappropriate legislation on personal

data protection, including the U.S., have also not been complied with. In relation to the fight against terrorism, the relevant processing of personal data has legal basis neither in the EU legislation nor in any binding international agreement between the EU and the U.S.
In its conclusions, WP 29 suggests that immediate steps be taken in order to resolve the current state of affairs and to cease violation of law. It expressed its opinion that responsibility in this matter was borne jointly by the SWIFT company and the financial institutions; however, the respective responsibilities are not equal. The main measures should be concerned primarily with the main responsible person – i.e. the data controller, the SWIFT company. Even though the banks founded the company, for a long period of time the newly acceding banks and financial institutions have not had any direct influence on its activities and, in a vast majority of cases, they are unable to control its activities and they do not make decisions on the nature and manner of services provided. A certain influence on its activities and, consequently, a certain degree of responsibility, is borne by the central banks of the G-10 countries and, particularly, by the National Bank of Belgium, given its involvement in the control bodies and, therefore, the ability to indirectly influence the activities of the company. Thus, the fundamental responsibility on the part of SWIFT for the transfer of data to the U.S. is unquestionable.

The Office for Personal Data Protection has not confined itself to mere monitoring of foreign developments. In July 2006, the President of the Office wrote a letter to the Governor of the Czech National Bank, where he informed him of this issue and requested his cooperation in obtaining further information. An official notice was sent to the Ministry of Finance of the Czech Republic in November 2006 and, at request, information containing evaluation of the matter was also provided to other authorities, namely the Ministry of Foreign Affairs and the Ministry of Interior of the Czech Republic. An inspection concerned with several banks was also initiated in 2006 within the competence of the Office, as an independent supervisory body, on the basis of a decision of the President of the Office; the inspection was directed by inspector Ing. Jan Zapletal. The objective of the inspection was to verify whether or not law had been breached in processing of personal data of the banks' clients in relation to the transfer of those data to the "SwiftNet Fin" system and, if such violation had indeed occurred, to adopt measures to cease and remedy such violation.
Although the inspection pursued by the Office for Personal Data Protection in selected banks has not yet been formally completed, it can be stated that the controlled entities have not breached the law from the viewpoint of processing of their clients' personal data that are part of the records of interbank transactions transferred abroad and, subsequently provided by the SWIFT company to the U.S. authorities within the fight against terrorism. The agreements between the control entities and the SWIFT company do not include any provisions whatsoever indicating that the records could be used for other purposes that are incompatible with the commercial purposes, for which the data are processed by the Czech banks and transferred abroad. The controlled banks mostly transfer their records containing personal data within the EU, or the European Economic Area, except for information on payments in currencies of countries outside this area; this information is first provided to a bank in the relevant "third" country. However, the clients are informed of this principle within the general terms and conditions related to the use of the "third" country currency. No restriction may prevent free flow of personal data within the EU/EEA for reasons connected with personal data protection. This is clearly stipulated by aforementioned Directive 95/46/EC in its Art. 1 (2), as well as by Article 27 (1) of Act No. 101/2000 Coll., on personal data protection and on amendment to some laws, as amended.

Finally, it must again be stressed that the responsibility for the current practice is borne particularly by SWIFT which transfers personal data to the U.S. and provides the data to the U.S. authorities. A certain degree of co-responsibility may also be perceived on the part of the financial institutions involved in SWIFT's control mechanisms, i.e. the central banks of the G-10 countries headed by the National Bank of Belgium. Indeed, those entities should be

required to seek a remedy and bear any appropriate sanctions. It is also likely that a future solution could lie in negotiations between the EU institutions and the U.S. authorities, aimed at establishing a legal basis for data transfers to the U.S. within an international agreement. However, while this would not change the current practice, certain contractual guarantees would be obtained from the U.S. authorities with respect to management of personal data.

However, the Office for Personal Data Protection believes that the clients of banks and financial institutions, as well as the general public, should at least be informed of this issue, which is indeed the objective of this press release.

In Prague, on January 25, 2007