The global provider of secure financial messaging services

Search swift.com Search





**Related Pages**

Previous statements and stories on compliance

# Compliance

## In Compliance

### Data Protection Policies

SWIFT has decided to enhance its contractual documentation and to improve transparency with respect to the processing of message and traffic data. In doing so, SWIFT has been assisted by a working group of data protection and compliance experts from European and non-European SWIFT users. In December 2008, the Belgian data protection commission concluded that SWIFT complied with all applicable Belgian data protection legislation.

### UST Subpoenas

After the attacks of September 11, 2001, the US Treasury Department (UST) launched the Terrorist Finance Tracking Program (TFTP). The TFTP program is ongoing and since the implementation of the new Distributed Architecture SWIFT receives and complies with valid and enforceable subpoenas for data located in its US Operating Center.

### Fighting illegal financial activities

Given its importance in the financial community, SWIFT cooperates in good faith with authorities in the fight against illegal activities.

About SWIFT
Company information
Community
Corporate Social Responsibility
Publications
Careers at SWIFT
Partner Corner
Press room
Legal
Corporate matters
SWIFT contracts
Trademark guidelines
SWIFTStandards IPR policy
Compliance

Related Pages

Previous statements and stories on compliance

# Data Protection Policies

SWIFT has decided to enhance its contractual documentation and to improve transparency with respect to the processing of message and traffic data. In doing so, SWIFT has been assisted by a working group of data protection and compliance experts from European and non-European SWIFT users.

The results from this work are published below.

### SWIFT Data Retrieval Policy

The SWIFT Data Retrieval Policy sets out SWIFT's policy on the retrieval, use, and disclosure of traffic and message data. This policy existed already, but has been enhanced to provide additional transparency.

### SWIFT Personal Data Protection Policy

The SWIFT Personal Data Protection Policy sets out the roles and responsibilities of SWIFT, the SWIFT community, and its customers with regard to the processing of personal data. Such roles and responsibilities were previously governed by the SWIFT General Terms and Conditions and other contractual documents, and are now consolidated in one single policy.

### SWIFT Safe Harbor Policy

The SWIFT Safe Harbor Policy provides an adequate level of protection for SWIFT's mirroring of data in its US Operating Centre. This policy specifically covers personal data contained in message data that relate to individuals resident of European Economic Area ("EEA") Member States or from Switzerland or that are sent by SWIFT customers established in one of the EEA Member States or Switzerland.

### Frequently Asked Questions

This document answers the most frequently asked questions on SWIFT's data processing activities and related data protection

matters.

The SWIFT Security Control Policy, to which some of these documents refer, can be found here.

The SWIFT General Terms and Conditions, to which some of these documents refer, can be found here.

About SWIFT
Company information
Community
Corporate Social Responsibility
Publications
Careers at SWIFT
Partner Corner
Press room
Legal
Corporate matters
SWIFT contracts
Trademark guidelines
SWIFTStandards IPR policy
Compliance

External Links
www.consilium.europa

# UST Subpoenas

Shortly after the September 11, 2001 attacks, the U.S. Treasury Department (UST) initiated the Terrorist Finance Tracking Program (TFTP). Under the TFTP, the Treasury Department issues administrative subpoenas for terrorist-related data.

SWIFT's US Operating Center falls under this program and must comply with subpoenas served from time to time by the UST's Office of Foreign Assets Control (OFAC).

These subpoenas require SWIFT to provide the UST with certain financial transaction records (in the form of SWIFT messages) which are located in SWIFT US Operating Center, to be used exclusively for counterterrorism purposes. The TFTP is ongoing and since the implementation of SWIFT's new Distributed Architecture infrastructure at the beginning of 2010, SWIFT receives requests to provide data located in the US. Intra-European zone messages are no longer processed and stored in SWIFT's US Operating Center.

On 28 June 2007, the UST transmitted to the Council Presidency of the European Union and to the European Commission a set of representations that describes the controls and safeguards governing the handling, use and dissemination of subpoenaed data under the TFTP. These controls and safeguards ensure that the subpoenaed data, which are limited in nature, are used strictly for counterterrorism purposes, and that data are retained only for as long as necessary for counterterrorism purposes and that all data are maintained in a secure environment and properly handled

In February 2009, the European Commission confirmed that the United States Treasury has from the outset, respected the safeguards in the handling of personal data obtained from SWIFT under subpoena. Read more at Subpoenaed SWIFT message data is adequately protected.

In December 2008, the Belgian data protection commission (Commission belge de la Protection de la Vie Privée) had already

concluded that SWIFT complied with all applicable Belgian data protection legislation. Read more at SWIFT respects data protection legislation.

More details on the UST representations can be found on the site of the Council of the European Union and in the Official Journal of the European Union.

# Subpoenaed SWIFT message data is adequately protected

Eminent European person confirms UST controls and safeguards

Published 18 February 2009

Vice-President Barrot, in charge of Justice, Liberty and Security at the European Commission has confirmed that the United States Treasury (UST) has from the outset, respected the safeguards in the handling of personal data obtained from SWIFT under subpoena following the attacks of 9/11.

In March 2008, the European Commission announced it had designated **Judge Jean-Louis Bruguière** to undertake a review on behalf of the European Union in respect of the procedures governing the handling, use, and dissemination of personal financial data from the EU that is carried over the SWIFT network and obtained by the UST pursuant to the Terrorist Finance Tracking Programme (TFTP). Judge Bruguière presented his first report to the European Commission in January 2009, which the Commission presented to the European Parliament's Civil Liberties Committee on 16 February 2009.

The report finds that the UST has been vigilant from the outset in respecting the safeguards in the handling of personal data included in the TFTP Representations and notably the strict counter terrorism purpose limitation. The report further finds that the TFTP has generated significant value in the fight against terrorism, notably in Europe.

This is testimony to SWIFT's determination to protect its customers' data in any circumstance. In December 2008, the Belgian data protection commission (Commission belge de la Protection de la Vie Privée) had already concluded that SWIFT complied with all applicable Belgian data protection legislation.

**This is the full EU announcement**

**EU Review of the United States 'Terrorist Finance Tracking Programme' confirms privacy safeguards**

In March 2008, the European Commission announced a review on behalf of the European Union in respect of the procedures governing the handling, use, and dissemination of financial transaction records from the EU which are carried over the SWIFT network and obtained by the U.S. Treasury Department pursuant to subpoenas issued in support of the Terrorist Finance Tracking Programme (TFTP). Judge Bruguière, designated by the Commission to undertake the review, prepared a first report to Vice-President Barrot.

Vice-President Barrot, in charge of Justice, Liberty and Security, presented today the findings to the European Parliament's Civil Liberties Committee and declared: "I am pleased to confirm that the United States Treasury Department has been vigilant from the outset in respecting the safeguards in the handling of personal data included in the TFTP Representations which we were able to negotiate with them back in 2007 and notably the strict counter terrorism purpose limitation. The TFTP has generated significant value in the fight against terrorism, notably in Europe".

The review focused particular attention on the core undertakings set out in the TFTP Representations, namely that SWIFT data are used exclusively for counter terrorism purposes; that the Treasury ensures that subpoenas are narrowly focused; that searches against the TFTP database are targeted and designed to minimise extraction of data; that appropriate measures are in place to identify and delete data which are no longer considered necessary for the fight against terrorism; and that necessary physical and logical systems exist to ensure the security of subpoenaed data.

The Report demonstrates that the United States Treasury Department has implemented significant and effective controls and safeguards which ensure respect for the protection of personal data subpoenaed for the purpose of the TFTP. Following his review of the TFTP and its surrounding privacy-related safeguards, Judge Bruguière formulated a series of recommendations to ensure that these measures are continued and, where possible, enhanced.

As a result of the information Judge Bruguière has had access to during discussions with the Treasury Department, it can be concluded that the TFTP has generated since its implementation and continues to generate, significant value for the fight against

terrorism in the United States, in Europe and beyond.

After the 11 September 2001 terrorist attacks the U.S. Treasury Department developed the TFTP for the investigation, prevention and prosecution of terrorism. Under the TFTP the Treasury Department has served administrative subpoenas on the Society for Worldwide Interbank Financial Telecommunication (SWIFT). These subpoenas require SWIFT in the U.S. to transfer a limited subset of message data held on its U.S. server to the Treasury Department where they may be used for counter terrorism purposes regarding suspected individuals or entities. In June 2007 the Treasury Department gave a set of unilateral commitments ("Representations") to the European Union regarding the controls and safeguards governing the handling, use and dissemination of data under the TFTP.

The Representations address EU data protection concerns and were published in the Official Journal in July 2007[1] and in the U.S. Federal Register in October 2007. The Representations allow the Commission to designate an "eminent European person" to assess whether the U.S. Treasury Department is implementing the TFTP in accordance with its Representations. The Commission announced the designation of Judge Bruguière for this purpose in March 2008.

It had to be confirmed whether the TFTP is implemented consistent with the Treasury Department’s representations for the purpose of verifying the protection of EU-originating personal data. The TFTP Representations state that an annual report will be delivered to the European Commission which in turn will present the findings of the report to the European Parliament and Council.

The global provider of secure financial messaging services

Search swift.com Search

About SWIFT | Solutions | Ordering | Support | Training | Events | Contacts

About SWIFT ▸ Legal ▸ Compliance ▸ Fighting illegal financial activities

Customer log in


- About SWIFT
- Company information
- Community
- Corporate Social Responsibility
- Publications
- Careers at SWIFT
- Partner Corner
- Press room
- Legal
  - Corporate matters
  - SWIFT contracts
  - Trademark guidelines
  - SWIFTStandards IPR policy
  - Compliance

External Links

www.fatf-gafi.org


# Fighting illegal financial activities

Cooperating in the global fight against abuse of the financial system for illegal activities

SWIFT is solely a carrier of messages between financial institutions. The information in these messages is issued and controlled exclusively by the sending and receiving institutions. SWIFT does not hold assets nor manage accounts on behalf of customers. It does not clear or settle transactions.

Given its importance in the financial community, SWIFT cooperates in good faith with authorities in the fight against illegal activities.

**1. Responsibilities** - It is SWIFT policy that its services should not be used to facilitate illegal activities. Users are urged to take all reasonable steps to prevent any misuse of the SWIFT system.

**2. Cooperation** - SWIFT has a history of cooperating in good faith with authorities such as central banks, treasury departments, law enforcement agencies and appropriate international organisations, such as the Financial Action Task Force ( FATF*), in their efforts to combat abuse of the financial system for illegal activities. The conditions under which SWIFT complies with requests from authorities to produce data and informs its customers are set forth in the SWIFT Data Retrieval Policy.

**3. No comment policy** - Due to the sensitive nature of the contacts with authorities and due to non-disclosure or other legal requirements, SWIFT does not comment on them.

The challenge facing the financial industry is to implement measures that prevent illegal behaviour without penalising the efficient processing of legitimate financial transactions. SWIFT is fully committed to doing its part to address this challenge and remains committed to its policy of cooperation to fight illegal activities within the scope of its activity.

* The FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a “policy-making body” created in 1989 that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. For more information, see the FATF website.

About SWIFT
Company information
Community
Corporate Social Responsibility
Publications
Careers at SWIFT
Partner Corner
Press room
Legal
Corporate matters
SWIFT contracts
Trademark guidelines
SWIFTStandards IPR policy
Compliance

External Links

www.swiftcommunity.n
www.swiftcommunity.n
www.sibos2009.com

# Privacy Statement – August 2008

## Introduction

At SWIFT, we are committed to protect and respect your personal data.

This Statement explains how we use personal data collected from you on our websites. Our websites include:

- www.swift.com
- www.swiftcommunity.net (with its own Terms of Use confirming this Statement)
- our annual Sibos website, available at www.sibos[year].com (currently http://www.sibos2009.com/), and
- other URLs that redirect to www.swift.com.

We invite you to carefully read this Statement to understand our data processing practices.

For the purpose of the Belgian Act on Privacy Protection in relation to the Processing of Personal Data of 9 December 1992 (the Belgian Act), the data controller for personal data collected on our websites is S.W.I.F.T SCRL, Avenue Adèle, 1, 1310 La Hulpe, Belgium ('SWIFT' or 'We' in this Statement).

We may modify this Statement from time to time. Please check it periodically for changes, in particular when you submit personal data on our websites.

This Statement only applies to the processing of personal data collected by us on our websites. Our other data processing activities are covered by other SWIFT policies. They are:

- The SWIFT Personal Data Protection Policy: it explains how we process our customer contact details (when collected on our websites - this part is common to this Statement - or on paper) and personal data that our customers encapsulate in SWIFT

messages or files (“message data”). Where relevant for the purposes of this Statement, we will explicitly refer to that Policy.
- The SWIFT Safe Harbor Policy: it explains how we mirror message data in our US Operating Centre. It is not relevant for the purposes of this Statement.
- The SWIFT Data Retrieval Policy: it explains how we retrieve, use, and disclose message and traffic data. It is not relevant for the purposes of this Statement.

**SWIFT Purposes**

We process personal data collected on our websites for the following purposes (together “SWIFT Purposes”):

- SWIFT governance
- The provision of SWIFT services and products
- Recruitment
- Organisation of Sibos and other events
- Newsletters and other customer communications
- The operation of our websites (IP addresses, cookies, web acceleration)

More information on the use of your personal data (as a SWIFT customer) for SWIFT governance and for the provision of SWIFT services and products is available in the SWIFT Personal Data Protection Policy.

More information about the use of your data for the other purposes is given below.

**Recruitment**

When you use our online recruitment tool, we collect personal data relating to the position you apply for, such as your name, home or business address, e-mail or other contact details, and other relevant personal data. We also require potential candidates to submit their résumés online.

We do not require any 'sensitive' data in our online recruitment process. We therefore kindly request you not to communicate any personal details revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or

sex life, litigation or judicial convictions. If you nevertheless provide us with such sensitive data, you agree that we may process it for our recruitment purposes.

We will process your data for the sole purpose of assessing your application. We will keep all your data confidential. We will not share your data with third parties outside the SWIFT group, with the exception of recruitment counsels and other processors acting on our behalf.

You may always delete your data by using your login and password.

**Sibos and Other Events**

When you register for Sibos or other events, we collect personal data related to your participation to the event.

We process your data for purposes relating to event registration, administration, security management, accounting, records keeping, to offer event-related products (such as the Sibos Networkbook) and services (such as mySibos) and for conducting satisfaction surveys.

The list of participants is sent in advance of the event to the exhibiting companies to allow them to present their products and services directly to you, and may be used by us for our own advertising and marketing purposes. You may opt out of this list in the online registration process.

You may contact events-mailing.unsubscribe@swift.com to unsubscribe from the Sibos and other events mailing lists.

**Newsletters and Other Customer Communications**

We may use personal data that we collect on our websites to provide you with newsletters and to invite you to participate in customer consultations and satisfaction surveys.

We only send you newsletters, customer consultations or satisfaction surveys that relate to SWIFT services and products.

In each mailing, we remind you about your right to opt-out of our newsletters, customer consultations or satisfaction surveys mailing lists.

You may opt-out or unsubscribe from the above mailings at any time by sending an e-mail to:

- leave-supportnews@list.swift.com for all our SWIFTSupport newsletters
- customer.Survey.Generic@swift.com for all our customer consultations and satisfaction surveys
- the unsubscribe e-mail address specific for each regional training newsletter (for example leave-north-america_training@info.swift.com for the North American newsletter), or to training.newsletter@swift.com in case of difficulties to retrieve the regional unsubscribe e-mail address.

Some of these newsletters and communications are sent to you on our behalf by suppliers specialised in mass mailings. We request those suppliers to provide us with the appropriate data protection and data security commitments (see 'Sharing Data' section below).

**Operation of our Websites**
**IP Addresses**

When you browse our websites, you do so anonymously. For our internal purposes, we may use IP addresses (the Internet address of your computer) stored in web logs to generate aggregate statistics on surf behaviour, such as traffic patterns and time spent on a page.

**Cookies**

Cookies are small pieces of information that are stored by your browser on your computer's hard drive or in your browser memory. We use cookies for authentication purposes (for example to access the secure area of www.swift.com ), to track user sessions (for example login information on both the secure and public areas of www.swift.com ), to repopulate fields (for example to access the Sibos Exhibitor Guide), or to track online acceptance (for example to track acceptance of the disclaimer of our translation service over the last 24 hours) or language preference.

The information stored with cookies may include your name, first name, registration number on www.swift.com , language preference, login ID, and IP addresses. Cookies stored in your browser memory are deleted when closing your browser.

**Web Acceleration Services**

For purposes of accelerating the consultation of our websites, we use the services of a supplier specialised in web acceleration services.

This requires caching the content of our websites on a substantial number of servers worldwide.

This supplier only processes data on our instructions, provides sufficient guarantees in respect of technical and organisational data security measures, and has committed to notify us in case of a security breach compromising your personal data (see also 'Sharing Data' section below).

**Data Security**

We are committed to protect your personal data against accidental or unlawful destruction, accidental loss, alteration, and unauthorised disclosure or access.

Please be aware that we cannot ensure the security of your data on your computer or during transmission over the Internet. In this regard, we advise you to take every possible precaution to protect personal data stored on your computer and transiting on the Internet.

**Data Submitted on Behalf of Someone Else**

When you provide us with personal data relating to someone else, please make sure to collect and supply such personal data in accordance with local applicable law.

For example, you may have to inform that other person about parts of this Statement in order to comply with local applicable law.

**Your Rights**

With regard to personal data collected on our websites, you may use the e-mail addresses provided in this Statement to:

- exercise your access and correction rights
- object to the processing for direct marketing purposes

We will handle all requests with care and diligence, and take corrective actions in accordance with the Belgian Act.

**Privacy Officer**

The SWIFT Privacy Officer carries out internal supervision in connection with our responsibilities under this Statement.

You may exercise your rights and address any questions to the Privacy Officer:

- by letter to S.W.I.F.T. SCRL, attention of Privacy Officer, Avenue Adèle 1, 1310 La Hulpe, Belgium
- by e-mail to privacy.officer@swift.com.

**Sharing Data**

We will not allow third parties to use your personal data for their own purposes without your consent.

When required for the SWIFT Purposes, we may share your data with other offices in the SWIFT group (see the SWIFT Offices page), carefully selected suppliers, or other selected third parties (typically SWIFT partners or sub-contractors).

Before sharing your data, we require such third parties to only process your personal data on our instructions and to provide sufficient guarantees in respect of the technical and organisational security measures protecting the data processing activities.

Such SWIFT offices or third parties may be located in or outside the European Economic Area (EEA), including in countries that do not offer a level of data protection considered as adequate under the Belgian Act.

In the latter case, we ensure the lawfulness of such transfers by:

- agreeing with other SWIFT offices on the standard contractual clauses approved by the European Commission Decision 2004/915/EC of 27 December 2004
- agreeing with third parties on the most appropriate statutory, contractual, or self-regulatory basis (for example Safe Harbor adherence) to allow such transfers.

statement use