



SWIFT India Domestic Services Private Limited

Data Confidentiality and Protection Policy

December 18, 2015

Restricted to Board Directors, Employees and
Customers



Table of Contents

1	INTRODUCTION.....	3
2	ACCESS RETRIEVAL DISCLOSURE AND USE OF TRAFFIC AND MESSAGE DATA .	5
2.1	Principles of confidentiality and restricted purpose.....	5
2.2	Retention period and deletion of data	6
2.3	Protection of retrieved data	6
3	Personal Data	8
3.1	Principles of good practice for processing or collecting Personal Data.....	8
3.2	Rights of Individuals.....	8
3.3	Data collected by SWIFT India for its own purpose.....	8
3.4	Data collected by customers of SWIFT India	9
4	Processing, storing and replication of traffic and message data	10
4.1	Rules relating to processing and storing of Message Data.....	10
4.2	Rules relating to replication of Message Data	10



1 INTRODUCTION

This documents sets out SWIFT India Domestic Services Private Limited's ("SWIFT India") policy for the retrieval, use and disclosure by SWIFT India of Traffic and Message data.

This document also sets out the roles and responsibilities of SWIFT India and its customers with regard to the processing of Personal Data (defined below) that either SWIFT India collects for its own purposes or that SWIFT India customers collect as part of their use of the SWIFT India domestic messaging services ("Services").

Further, this document sets forth the rules for the processing, storing and replication of Traffic and Message Data in India (as defined below).

This policy forms an integral part of the contractual arrangements between SWIFT India and its customers for the provision of the SWIFT India's Services and should be read in conjunction with them.

This policy covers the:

- a) access, retrieval, disclosure and use of SWIFT India Traffic and Message Data. (see Section 2);
- b) processing of Personal Data. (see Section 3); and
- c) processing, storing and replication of Traffic & Message Data, (see Section 4).

Given SWIFT SCRL provides its intellectual property and operations services to SWIFT India for provision of domestic messaging services to its customers, SWIFT India shall ensure that all provisions in this policy shall equally apply to SWIFT SCRL. SWIFT India authorises SWIFT SCRL (as a service provider and licensor) to perform many acts to give effect to and execute any rules specified in this policy. SWIFT SCRL will support SWIFT India in observing local laws and regulations as may be deemed necessary by SWIFT SCRL.

The content messages remain the property of the sender and receiver, and are accessible by the sender and receiver. The content of messages will be accessible by SWIFT SCRL as described in this policy for the purpose of provision of monitoring and problem investigation only.

SWIFT India and its customers are obliged to comply with applicable laws and regulations. SWIFT India and its customers will inform each other in case they become aware of any developments regarding applicable data protection laws and regulations that may have a potential impact on SWIFT India's products and services. In such event, SWIFT India and the customers review and discuss such potential impact, through the most appropriate SWIFT India governance structures.

This policy shall be interpreted in accordance with Indian laws and the terms used in the policy shall have the meanings ascribed to them under Indian laws.



SWIFT India - Data Confidentiality and Protection Policy

Definitions:

- a) **“Collective Request”** means a request from an organisation (typically, a regulatory or supervisory authority, a market infrastructure, a financial industry group, or a customer advisory group) that requests SWIFT India to retrieve, use, or disclose Traffic or Message Data for purposes representing a legitimate collective interest (e.g., without limitation, to assess market practices, to assess financial risks related to the use of the SWIFT India services, or to improve the quality of SWIFT India standards and services). In such cases, SWIFT India reviews and assesses any such request. SWIFT India only accesses, retrieves, uses, or discloses Traffic or Message Data, in an aggregated and **anonymised** form, only if the requesting organisation demonstrates, to the reasonable satisfaction of the SWIFT India Board or its delegated body, that its request is legitimate.
- b) **“Anonymised data”** means data from which SWIFT India has removed any identification details relating to individuals or entities referred to in Message Data.
- c) **“Exceptional Requests”** means a third party request to access, retrieve, use and disclose Traffic or Message Data in the following exception circumstances:
 - i. In response to a Collective Request;
 - ii. To comply with a Mandatory Request.
- d) **“Information”** includes data, texts, images, sound, voice, codes, computer programme, software and database, micro film or computer generated micro fiche.
- e) **“Mandatory Request”** means a legally enforceable request, in whatever form, by a judicial, administrative, governmental, or other competent authority that has jurisdiction over SWIFT India, compelling SWIFT India to retrieve, use, or disclose Traffic or Message Data in its possession.
- f) **“Message Data”** refers to the internal content of the message or the file (typically, the payload of InterAct messages or the file of FileAct messages). To access Message Data, the related message or file must be retrieved, opened, and the contents, as applicable, decrypted.
- g) **“Personal Data”** refers to Sensitive Personal Data and Personal Information
- h) **“Personal Information”** means Information that identifies data subjects as an individual or is capable of doing so.
- i) **“Sensitive Personal Data”** means such Personal Information which consists of Information relating to:
 - Password;
 - financial information such as bank account or credit card or debit card or other payment instrument details;
 - physical, physiological and mental health condition;
 - sexual orientation;
 - medical records and history;
 - biometric information;



SWIFT India - Data Confidentiality and Protection Policy

- any detail relating to the above areas as provided to body corporate for providing service; and
 - any of the Information received under the abovementioned clauses by SWIFT India for processing, stored or processed under lawful contract or otherwise; and includes Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence by any court in such proceedings.
- j) **"SWIFT India Board"** means the board of directors of SWIFT India.
- k) **"SWIFT SCRL"** is a cooperative society under Belgian law and is a service provider and licensor to SWIFT India.
- l) **"Traffic Data"** refers to the information contained in the header or the trailer of the message or the file. Traffic Data typically includes external addressing and delivery elements (for example, the sender, receiver, message or request type, and message or file transfer history). By its very nature, Traffic Data does not contain data relating to individuals, nor does it allow the identification of individuals.

2 ACCESS, RETRIEVAL, DISCLOSURE AND USE OF TRAFFIC AND MESSAGE DATA

This section sets forth the principles and rules for the access, retrieval, disclosure and use of Traffic and Message Data stored in the SWIFT India computer systems (also known as Operating Centres or OPCs).

2.1 Principles of confidentiality and restricted purpose

Message and Traffic Data are confidential and their access, retrieval, disclosure and usage are restricted and are only authorised in the following circumstances:

- a) *Provision of SWIFT India products and services:* Message and Traffic Data can be accessed, retrieved, disclosed, and used for the provision of SWIFT India Services and related products (e.g. for billing purposes, or in connection with a claim against SWIFT India, its suppliers related to performance of SWIFT India's messaging Services)
- b) *At the request of the sending or receiving customer, including in case of claim between customers. For the purposes of this policy, any request by a Customer's regulator for access to their Traffic and Message Data in accordance with clause 12.2 of the General Terms and Conditions shall be deemed to be a customer request under this clause.*
- c) *To investigate or resolve problems with the provision of SWIFT India's services and products*



SWIFT India - Data Confidentiality and Protection Policy

- d) *At SWIFT India's initiative, Traffic Data* can be accessed, retrieved, disclosed and used, in aggregate form only and without revealing the sender's and the receiver's identification details, e.g. give data to customer about its own traffic (both sent and received traffic).
- e) In case of **"Exceptional Requests"**
- i. **Collective Request:**
SWIFT India only discloses Traffic or Message Data in response to a legitimate collective request from an organisation, provided that this does not reveal the identity of customers, individuals, other third parties, or their business relationships.
 - ii. **Mandatory Request:**
SWIFT India may be subject to Mandatory Requests issued in India where it operates. This policy or, more generally, SWIFT India's obligations of confidentiality to customers as set out in its contractual documents, shall not be construed as preventing SWIFT India from retrieving, using or disclosing Traffic or Message Data as necessary to comply with a Mandatory Request.

In case of Mandatory Requests, to the extent legally required, Traffic or Message Data will not be shared with the requestor without first discussing with the competent regulator or formally asking the requestor to discuss the request with the regulator first.

SWIFT India reviews and assesses Mandatory Requests in accordance with this policy in order to determine whether or not it is compelled to comply with such Mandatory Requests. Such procedures include discussions with the regulator, the approval to comply with a Mandatory Request by the SWIFT India Board or its delegated body. Such approval is based on substantiated assurance obtained from SWIFT India's legal counsel that the mandatory request is lawful and enforceable against SWIFT India.

2.2 Retention period and deletion of data

Message Data will be stored by SWIFT India for a limited period as defined in the applicable service description as the "Contractual Retention Period" and deleted thereafter. SWIFT India may be required to preserve the Message Data beyond the Contractual Retention Period - when required by law or in the context of litigation.

2.3 Protection of retrieved data

a) **Data in SWIFT India's possession:**

SWIFT India and its suppliers shall ensure the confidentiality and integrity of the retrieved data in its possession.

Only authorised staff, agents or sub-contractors that are bound by appropriate contractual confidentiality obligations will have access to Message Data.

SWIFT India and its suppliers will destroy all retrieved copies of Message Data once the retrieved Message Data has been made available to the



SWIFT India - Data Confidentiality and Protection Policy

requesting customer, or once the purpose for which the data was retrieved in accordance with this policy has been achieved.

It is clarified that the Message Data will be in possession of SWIFT India and not with its suppliers, unless provided for under this policy.

b) Data supplied to customers:

The protection of Traffic or Message Data retrieved by SWIFT India at the customer's request is the sole responsibility of the customer once the data has been made available to the authorised recipient designated by the customer.

c) Data shared with SWIFT India suppliers:

In the exceptional circumstance that SWIFT India (or its suppliers) needs to share a copy of the Message Data for purposes of problem investigation or resolution, SWIFT India takes the following actions:

- i. ensure that the disclosure of the Message Data to such supplier has been duly authorised by SWIFT India management having regard to the circumstances;
- ii. make the Message Data available to such authorised supplier in an encrypted manner;
- iii. ensure that such supplier is bound by no less stringent obligations of confidentiality and data protection than those applicable to SWIFT India. In particular, SWIFT India must seek the supplier's express commitment in writing to do the following:
 - only grant the supplier's authorised staff, agents, or suppliers access to the Message Data on a need-to-know basis
 - confirm in writing, upon completion of the investigation or the resolution of the problem, the destruction of all copies of Message Data or any work product which may contain the same Message Data.

d) Data disclosed based on a collective request:

When disclosing Traffic or Message Data in response to a legitimate collective request, SWIFT India notifies the requesting organisation or authority of the confidential nature of the data and requests such organisation or authority to preserve the confidentiality of the Traffic or Message Data.

e) Data disclosed based on a Mandatory Request:

When disclosing Traffic or Message Data in response to a Mandatory Request, SWIFT India takes the following actions:

- i. notify the authority issuing the Mandatory Request of the confidential nature of the data, of SWIFT India's obligation to inform its customers about the disclosure of their data, and of any other protections that may apply to the data and of which SWIFT India may be aware (typically, protections resulting from relevant data protection principles and laws);
- ii. request such authority to preserve the confidentiality of the data and, as the case may be, to preserve such other protections;



SWIFT India - Data Confidentiality and Protection Policy

- iii. unless prevented by confidentiality or other requirements under applicable law, as acknowledged by the SWIFT India Board or its delegated body, inform the customers that have sent or received the data of such disclosure, prior thereto. SWIFT India will determine the most appropriate means of such notification in the light of the circumstances and all obligations applicable to SWIFT India, including potentially conflicting information and non-disclosure requirements. If SWIFT India is prevented by confidentiality or other requirements under applicable law to inform the customers concerned prior to such disclosure, then SWIFT India informs them without delay once such information becomes reasonably practicable or permitted. SWIFT India reassesses on a regular basis whether such information can be provided.

3 PERSONAL DATA

This section sets forth the rules for the processing of Personal Data that SWIFT India collects for its own purposes or that SWIFT India customers collect as part of their use of SWIFT India Services.

- 3.1 Principles of good practice for processing or collecting Personal Data
SWIFT India will comply with the following principles while processing Personal Data. The customers of SWIFT India will comply with these principles when collecting Personal Data. These principles provide that the Personal Data must be:
 - i. Processed fairly and lawfully;
 - ii. Processed for limited purposes and in an appropriate way;
 - iii. Adequate, relevant and not excessive for the purpose;
 - iv. Accurate;
 - v. Not kept longer than necessary for the purpose, except in certain exceptional cases described herein;
 - vi. Processed in line with data subject's rights;
 - vii. Secure; and
 - viii. Not transferred to people or organisations situated in countries without adequate protection.

- 3.2 Rights of Individuals
The data subjects have the following rights:
 - i. Requesting access to any data held about them by a data controller;
 - ii. Preventing the processing of their data for direct-marketing purposes;
 - iii. Asking to have inaccurate data amended or removed; and
 - iv. Preventing processing that is likely to cause damage or distress to themselves or anyone else.

- 3.3 Data collected by SWIFT India for its own purpose



SWIFT India - Data Confidentiality and Protection Policy

SWIFT India may process Personal Data (Sensitive Personal Data and/or the Personal information), on individuals collected by SWIFT India for purposes relating to the provision of the SWIFT India services and products or relating to SWIFT India governance (the “**SWIFT India Purposes**”).

The SWIFT India Purposes include the following:

- the admission as a SWIFT India customer, and the ongoing management of such customer relationship;
- the development, subscription, deployment, provision, support, promotion, and invoicing of the SWIFT India services and products;
- the registration and management of the SWIFT India customers' security officers required for the use of SWIFT India services and products (a security officer is the person that handles security matters for the SWIFT India customer);
- the subscription, deployment, provision, support, promotion, and invoicing of SWIFT India services and products;
- the registration and management of the customers' representatives that are active in SWIFT India advisory and working groups; or
- accounting, records keeping, customer information, and claims management.

The Personal Data collected typically include contact details of individuals provided by the customer (such as Personal Data relating to employees, officers, or directors of the customer).

3.4 Data collected by customers of SWIFT India

Customers of SWIFT India collect Personal Data from their clients and supply them to SWIFT India as part of their use of the SWIFT India Services. For example, SWIFT India customers may include Personal Data (such as name, address, and account number of an instructing or beneficiary party in a payment transaction) in the messages or files they send.

SWIFT India has no relationship with these individuals. Only SWIFT India customers know their clients and employees, have a contractual relation with them, and may collect their Personal Data.

Only SWIFT India customers determine the purposes for which the Personal Data of their clients may be processed and the most suitable means to do so. SWIFT India customers retain the exclusive right of controlling such Personal Data.

SWIFT India's responsibilities:

- (i) **Confidentiality:** SWIFT India will keep Message Data (that may include Personal Data) confidential and shall only use such data for providing the SWIFT India messaging services and in line with this policy.
- (ii) **Processing on instruction:**
With regard to Personal Data provided by SWIFT India customers, SWIFT India:
 - only processes such Personal Data on instructions of the SWIFT India customers;



SWIFT India - Data Confidentiality and Protection Policy

- does not retrieve, use, or disclose Message Data (which may contain Personal Data) except as set out in **section II above**
- does not process Personal Data contained in Message Data for other purposes;
- has implemented appropriate technical, physical, and organisational security measures that are designed to ensure the security of Message Data (which may contain Personal Data), and to protect such Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against other anticipated threats or hazards and relevant unlawful forms of processing.

SWIFT India customers' responsibility:

(i) **Provide instructions to process**

By subscribing to the SWIFT India Services and by providing Personal Data as part of their use thereof, SWIFT India customers instruct SWIFT India:

- to process such Personal Data in accordance with the SWIFT India contractual terms, this policy and any other relevant service documentation; and
- to apply the security measures as described above and in the service documentation applicable to such processing.

(ii) **Compliance with local applicable laws**

When providing Personal Data to SWIFT India, SWIFT India customers must collect such Personal Data for the relevant purposes in compliance with local applicable laws. In doing so and where relevant, SWIFT India customers must take the following points into account (amongst others):

- the technical and organisational security measures of the SWIFT India messaging services; and
- **Section 2 – ACCESS RETRIEVAL DISCLOSURE AND USE OF TRAFFIC AND MESSAGE DATA** of this policy

4 PROCESSING, STORING AND REPLICATION OF TRAFFIC AND MESSAGE DATA

The section sets forth the rules for replication, local processing and storage of Message Data in the 2 (two) OPCs.

- 4.1 Rules relating to processing and storing of Message Data
SWIFT India will process and store domestic participant data, i.e. Message Data, exchanged between customers within the 2(two) Indian OPCs alone.
- 4.2 Rules relating to replication of Message Data
SWIFT India will replicate the domestic participant data only between the 2(two) Indian OPCs.



Legal Notices

Copyright

SWIFT India Domestic Services Private Limited © 2015. All rights reserved.

You may copy this publication within your organisation. Any such copy must include these legal notices.

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version from SWIFT India Domestic Services Private Limited.

Translations

The English version of SWIFT India documentation is the only official and binding version.

Trademarks

SWIFT is the trademark of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: SWIFT, the SWIFT logo, the Standards Forum logo, 3SKey, Innotribe, Sibos, SWIFTNet, SWIFTReady, and Accord.

All other products, services, or company names that may be mentioned in this document are trademarks or registered trademarks of their respective owners.