SWIFT 3SKey

Privacy Policy

This document sets out the roles and responsibilities of SWIFT and its customers with regard to the processing of personal data in the context of the 3SKey Solution. It is an addendum to the 3SKey Tokens Terms and Conditions and the 3SKey Service Description.

January 2022

Table of Contents

Preface

About this document

This Privacy Policy describes the processing of Personal Data in the context of the SWIFT Secure Signature Key services, including the 3SKey digital keys and their functionalities (the "**3SKey Solution**") It sets out the roles and responsibilities of SWIFT and its Customers in the context of the 3SKey Solution.

The present Privacy Policy must be read in conjunction with the 3SKey Tokens Terms and Conditions and the 3SKey Service Description. It forms an integral part of the contractual arrangements between SWIFT and its Customers for the access and use of the 3SKey Solution.

Capitalized terms used but not defined in this Privacy Policy have the meaning given to them in the 3SKey Tokens Terms and Conditions, the 3SKey Service Description, and the SWIFT Glossary.

Related documentation

The following documents are of relevance to this 3SKey Privacy Policy:

- *SWIFT Glossary (available on the SWIFT website)*
- *3SKey Tokens Terms and Conditions*
- *3SKey Service Description (available on the 3SKey portal at www.3skey.com)*

1. Introduction

Overview

The Protection of Personal Data is very important to SWIFT, as confidentiality of data touches upon the core of its activities.

SWIFT's customers, when they interact with their corporate clients through electronic banking channels, may need to assess whether payment instructions have been approved by the competent individual(s) on the side of the client.

SWIFT introduced the 3SKey Solution to simplify this process, enhance security and reduce the operational risks and costs for the organizations concerned. With this solution, SWIFT supplies digital keys to Customers and manages the activation of these digital keys. The digital keys replace the current hardware tokens that are not adapted to recent technological developments such as mobile banking and cloud virtualized environments. Customers offer these digital keys to their clients (i.e., the 3SKey Users), who can use them to authentify transactions.

As part of the provision of this solution, SWIFT (i) manages and operates the SWIFT Public Key Infrastructure ("**PKI**"), which generates the credentials (i.e., a certificate and private key) that can be used to sign transactions; and (ii) provides a portal for 3SKey Users to activate and manage their keys (the "**3SKey Portal**"). In the context of the 3SKey Solution, Customers and SWIFT may process information relating to identified or identifiable individuals ("**Personal Data**").

2. Scope

Scope of the 3Skey Privacy Policy

This Privacy Policy (the "**Policy**") applies to the processing of Personal Data by Customers and SWIFT in the context of the 3SKey Solution. SWIFT and the Customers agree to process Personal Data as described in this document and in compliance with applicable data protection laws, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), and any applicable national legislation implementing the GDPR (together referred to as "**Data Protection Law**").

Categories of individuals

- Customers use the 3SKey Solution to provide their clients (i.e., the 3SKey Users) with a digital key solution for signing and authentifying transactions. For this purpose, SWIFT and Customers may process Personal Data relating to administrators and authorized signatories at Customers and 3SKey Users (i.e., individuals at banks and corporate users that use the 3SKey Solution).

Types of personal data

SWIFT and its Customers may process the following types of Personal Data:

- Unique ID (i.e., unique identifier generated by SWIFT for the given 3SKey physical or digital key, and used by the Customers to associate the 3SKey Users with the credentials generated by the SWIFT PKI).

- Name, email address and phone number of the 3SKey User's representative who uses the 3SKey Solution, as provided by the 3SKey User's representative.

Data disclosures

SWIFT and its Customers may disclose Personal Data to their affiliates and vendors as necessary for the purposes set out in Section 3 below. SWIFT will process and store any Personal Data in the context of the 3SKey Solution in the European Economic Area or Switzerland.

3. Purposes

SWIFT and its Customers have jointly determined the purposes for which they may process Personal Data in the context of the 3SKey Solution.

SWIFT may process Personal Data for the purpose of operating the 3SKey Solution, including managing the PKI and 3SKey Portal, and ensuring the security of the 3SKey Solution. Customers may process Personal Data for the purpose of providing the 3SKey Solution to the 3SKey Users. SWIFT and its Customers process Personal Data for their legitimate interest of enhancing security in electronic payments.

SWIFT and its Customers will not retain Personal Data for longer than necessary to fulfill their respective processing purposes.

4. Roles of the Parties

SWIFT and its Customers act as co-controllers when they process Personal Data for the above purposes. Their roles with regard to the 3SKey Solution are as follows:

- Customers offer the 3SKey Solution to the 3SKey Users and have a direct relationship with them.
- SWIFT manages the PKI and the activation of the digital key.

Based on these respective roles, this 3SKey Privacy Policy further allocates the responsibilities between SWIFT and Customers regarding the processing of Personal Data as follows:

- Customers are responsible for the data protection obligations that require direct contact with individuals (such as notice requirements, dealing with individuals' rights and data breach notification obligations towards impacted individuals).
- SWIFT is responsible for obligations that relate to the management of the 3SKey Solution, and that do not require direct contact with individuals.

5. Roles and Responsibilities

General principles

Each co-controller is only responsible for compliance with applicable Data Protection Law and with the obligations and responsibilities assigned to it in accordance with this Policy, in particular this Section 5.

Each co-controller's liability is limited to its own acts or omissions, and no co-controller will be jointly liable with another co-controller for that other co-controller's violation of applicable Data Protection Law or its obligations under this Policy. In particular, no co-controller will be liable for any loss or

damage resulting from, or attributable to, another co-controller's failure to comply with its obligations under this Policy.

Where a co-controller is made aware that an act or omission of another co-controller is or may cause the former to be in violation of applicable Data Protection Law or this Policy, it will first notify the other co-controller of the potential violation with a view to address the issue with the other co-controller. Both parties will cooperate fully with each other to take all reasonable and lawful efforts to mitigate the effects of, or to resolve, such violation, until a mutually acceptable solution is found.

Specific roles and responsibilities are allocated between the respective co-controllers as set out below.

5.1. SWIFT's Roles and Responsibilities

Compliance with applicable Data Protection Law

SWIFT ensures that it processes Personal Data in compliance with applicable Data Protection Law.

Management of the 3SKey Solution

As the party managing the 3SKey Solution, SWIFT must comply only with those specific obligations set out in this section that Customers cannot perform individually.

Data Storage

SWIFT hosts the 3SKey Solution on SWIFT's operating centres and grants 3SKey Users access to the 3SKey Portal for authentication purposes and signing of transactions.

Data security

SWIFT maintains appropriate technical and organisational measures to protect Personal Data it processes in the course of the provision of the 3SKey Solution against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access.

SWIFT has developed its information security practices in alignment with ISO27xxx industry standards as well as with relevant NIST SP800 publications. SWIFT reviews its security measures on a regular basis.

Rights of individuals

When an individual contacts SWIFT to exercise its data protection rights (including the right of access, rectification, erasure or restriction, data portability, consent withdrawal, the right to object to the processing, and rights relating to automated individual decision-making where applicable), SWIFT will advise that individual to direct its request to the Customer of which it (or its employer) is the client and who will respond to such request as set out below. SWIFT will provide this Customer with the necessary assistance in handling such requests.

In addition, every individual also has the right to submit a complaint with the competent data protection authority.

As SWIFT is established in Belgium, the competent data protection authority is the Belgian Data Protection Authority, Rue de la Presse 35, 1000 Brussels, Phone: +32 (0)2 274 48 00; Fax: +32 (0)2 274 48 35; E-mail: contact@apd-gba.be; website: https://www.dataprotectionauthority.be

Limited retention and deletion periods

SWIFT will retain and delete Personal Data in accordance with the retention and deletion periods set out in the service documentation, and will in any event not retain Personal Data for longer than is necessary for the purposes set out above.

Cooperate with enquiries from local authorities

Where a Customer is required to deal or comply with any assessment, enquiry, notice or investigation by a local data protection authority that relates to its contribution or use of Personal Data as part of its use of the 3SKey Solution, SWIFT will cooperate with reasonable and lawful requests for assistance of information to enable such Customer to respond to its local authority.

Data breach notification

SWIFT will notify the Customer and the Belgian Data Protection Authority, where required under applicable Data Protection Law, of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in connection with the 3SKey Solution ("**Personal Data Breach**"), provided that:

- SWIFT detects or is made aware of such Personal Data Breach;
- The Personal Data relating to clients of the notified Customer was impacted by such Personal Data Breach;
- The Personal Data Breach originates from the 3SKey Portal or other systems under SWIFT's control;
- SWIFT is not prohibited by applicable law, including statutory, regulatory, contractual or law enforcement requirements to notify the Personal Data Breach; and
- SWIFT will notify the Customer as soon as reasonably practical, with a view to allow the Customer to comply with the Personal Data Breach notification requirements under its own applicable law.

Provided that SWIFT has certainty regarding the facts related to the Personal Data Breach, SWIFT's Personal Data Breach notice will include the following:

- A summary of the incident that caused the Personal Data Breach (including the nature of the breach);
- The estimated date on which the Personal Data Breach occurred;
- The likely consequences of the Personal Data Breach;
- The measures taken or proposed to address the Personal Data Breach, including, where appropriate, the measures to mitigate its possible adverse effects;
- The categories and approximate number of Personal Data (records) impacted by the Personal Data Breach;
- The categories and approximate number of individuals to whom the impacted data relates.

SWIFT will cooperate with reasonable and lawful investigations that the Customer may carry out in relation to the Personal Data Breach.

Except to the extent prohibited by applicable statutory, regulatory or law enforcement requirements, SWIFT must obtain the approval of the concerned Customer prior to the publication or communication

of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mentions the Customer.

How to contact SWIFT

Any questions about SWIFT's responsibilities regarding the 3SKey Solution can be directed to your 3SKey Support contact.

Privacy or data protection related questions and requests can be addressed to:

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

SWIFT's Privacy Officer is authorized to carry out internal supervision in connection with SWIFT's responsibilities under this Policy.

5.2. Customers' Roles and Responsibilities

Compliance with applicable Data Protection Laws

Customers must, each with regard to the 3SKey Users that are their clients, comply with applicable Data Protection Law. In particular, Customers must comply with the obligations that require a direct contact with the 3SKey Users, as described below:

- Customers should ensure that the Personal Data relating to their clients is processed lawfully, fairly and in a transparent manner;
- Customers should inform their clients who are 3SKey Users about the processing of Personal Data as part of the 3SKey Solution, as described in this Privacy Policy;
- Customers should ensure that they have a legal basis for processing Personal Data in the context of the 3SKey Solution, and sharing the Personal Data relating to the 3SKey Users with SWIFT for the purposes of the provision of the 3SKey Solution.

Cooperate with enquiries from local authorities

Where SWIFT is required to deal or comply with any assessment, enquiry, notice or investigation from a data protection authority that relates to the processing of Personal Data as part of the 3SKey Solution, Customers will cooperate with reasonable and lawful requests for assistance or information from SWIFT to enable SWIFT to respond to such authority.

Rights of individuals

Customers must, in compliance with applicable Data Protection Law and where necessary with the collaboration of SWIFT, handle the 3SKey Users' requests to exercise individuals' rights of access, rectification, restriction, erasure, data portability, objection, consent withdrawal, and their rights relating to automated individual decision-making, as provided for under applicable Data Protection Law.

In case individuals exercise their right to object, their Personal Data will no longer be processed as part of the 3SKey Solution unless there are compelling legitimate grounds for this processing that override their interests or data protection rights, or if the processing is necessary for SWIFT's or the Customers' establishment, exercise or defence of legal claims.

Data breach notification

Customers must notify SWIFT of any Personal Data Breach in connection with the 3SKey Solution, provided that:

- The concerned Customer detects or is made aware of such Personal Data Breach;
- The Personal Data Breach relates to Personal Data relating to 3SKey Users that are clients of the concerned Customer; and
- The concerned Customer is not prohibited by applicable law, including statutory, regulatory, contractual or law enforcement requirements, to notify the Personal Data Breach.

For the avoidance of doubt, any Personal Data Breach that relates to the 3SKey Solution must be notified to SWIFT. Customers will notify SWIFT as soon as reasonably practicable, with a view to allow SWIFT to comply with the Personal Data Breach notification requirements under Belgian data protection law.

Provided that the concerned Customer has certainty regarding the facts related to the Personal Data Breach, the Customer's Personal Data Breach notice will include the following:

- A summary of the incident that caused the Personal Data Breach (including the nature of the breach);
- The estimated date on which the Personal Data Breach occurred;
- The likely consequences of the Personal Data Breach;
- The measures taken or proposed to address the Personal Data Breach, including, where appropriate, the measures to mitigate its possible adverse effects;
- The categories and approximate number of Personal Data (records) impacted by the Personal Data Breach;
- The categories and approximate number of individuals to whom the impacted data relates.

The concerned Customer will cooperate with reasonable and lawful investigations that SWIFT may carry out in relation to the Personal Data Breach.

Except to the extent prohibited by applicable statutory, regulatory or law enforcement requirements, the Customer must obtain SWIFT's approval prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mentions SWIFT.

When a Personal Data Breach on the side of the Customer or SWIFT is likely to result in a high risk to the data protection rights of the impacted individuals, the Customer will also notify this breach to such individuals without undue delay. This notification will include at least the following:

- A summary of the incident that caused the Personal Data Breach (including the nature of the breach);
- The name and contact details of the responsible data protection officer or other contact point on the Customer side where more information can obtained;
- The likely consequences of the Personal Data Breach;
- The measures taken or proposed to address the Personal Data Breach, including, where appropriate, the measures to mitigate its possible adverse effects.

The Customer will notify the impacted individuals as soon as reasonably practicable, in order to meet its own and SWIFT's Personal Data Breach notification requirements under applicable Data Protection Law.

Where required, the Customer will additionally ensure compliance with its own local Personal Data Breach notification requirements.

Customers should also comply with their own obligations of record keeping, performing data protection impact assessments and appointing a data protection officer, if and as required by applicable Data Protection Law.

Legal Notices

Copyright

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

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

Trademarks