SWIFT ENABLER PROGRAMME TERMS AND CONDITIONS
(Including Business Connect Solution)
(as of July 1st, 2023)

SIGNIFICANT CHANGES

This document represents a significant revision and merger of the SWIFT Enabler Programme Terms and Conditions and the SWIFT Business Connect Programme Terms and Conditions. The Enabler Programme and the Business Connect Programme have been merged and the Enabler Progamme, as described in this document, supersedes both the former Enabler Programme and Business Connect Programme. All participants under such programmes (as well as new participants under the Enabler Programme as described in this document) should review this document in its entirety, as it introduces changes to the previous versions of the Enabler Programme Terms and Conditions and the Business Connect Programme Terms and Conditions. These changes include, but are not limited to,
a change to the Business Connect Programme Terms and Conditions regarding the notice period relating to termination for convenience (see article 12.4).

PREFACE

(1) **SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION** ("**SWIFT**") is active in the field of secure financial messaging services and offers various services and products that support such messaging services or that are complementary to such messaging services. SWIFT wishes to facilitate the delivery of certain of its services to SWIFT customers through SWIFT Application Programming Interfaces (APIs). In addition, SWIFT will facilitate connectivity to its messaging services through the SWIFT's Alliance Cloud solution as per the Alliance Cloud Service Description (such facilitation of connectivity is referred to as the "**Business Connect Solution**"). In each case, registered providers (each referred to in this document as a "**Partner**") under the SWIFT Partner Programme will be involved in such facilitation. A Partner admitted by SWIFT into the Enabler Programme (as defined below), will be required to qualify for the Programme with respect to one or more of those SWIFT services provided through SWIFT APIs and/or the Business Connect Solution.

(2) Partner wishes to integrate or embed the Business Connect Solution and/or one or more SWIFT service(s) that may be accessed through SWIFT APIs (collectively the Business Connect Solution and such services are referred to as the "**SWIFT Services"**), as identified in the schedule furnished or to be furnished to Partner by SWIFT (the "**Partner Schedule**") into its own application, solution or middleware (the "**Partner Service"**) that Partner distributes to its customers, who are or will also be subscribing SWIFT customers in relation to the enabled SWIFT Services (collectively, the "**End Users"**). Unless the context clearly indicates otherwise, a reference herein to SWIFT Services means those SWIFT Services for which a particular Partner has been accredited and authorised by SWIFT to act as a distribution channel as part of this programme. In carrying out such role, Partner may also use Community API service(s) expressly defined by SWIFT, when and as authorised by SWIFT.

(3) This programme, in which a qualifying Partner enables (i) the consumption of SWIFT Services by End Users through SWIFT APIs (the "**SWIFT APIs**") corresponding to such services and/or (ii) connectivity to the SWIFT messaging network through the Business Connect Solution, on the one hand, and the Partner Service, on the other hand, is referred to as the "**Enabler Programme"**. Partners participating in the Enabler Programme and enabling the consumption of SWIFT Services through SWIFT APIs may implement and configure the SWIFT Software Development Kit (SDK) and/or SWIFT Microgateway, in addition to using the SWIFT API Gateway and SWIFT Developer Portal resources, to assist their solution development to interact with SWIFT APIs. Partners participating in the Enabler Programme will operate in a framework in which one or more of the following will apply, as appropriate and agreed by the parties: shared objectives as between SWIFT and Partner; tracked performance metrics for Partner participation; and defined benefits for Partners

exceeding programme objectives. More particularly, in the Enabler Programme, a Partner can either:

a. integrate/embed access to SWIFT Services into its own application or solution (the "**Business Application Model"**). In this case, a Partner enabling SWIFT Services through SWIFT APIs must satisfactorily request or call on the SWIFT APIs corresponding to the SWIFT Service(s) designated on the Partner Schedule, using the appropriate credentials, when the End User accesses and uses the integrated/embedded SWIFT Service(s); or

b. integrate/embed access to the SWIFT Service(s) in its middleware, which is connected to an End Users application or solution or a third-party application or solution (the "**API Concentrator Model"**). In this case, the End User's or a third party's application or solution (a "**Distribution Element"**) is associated with Partner's middleware in connection with distribution of the integrated/embedded SWIFT Services, and it (i) requests/calls upon Partner's APIs (which are an identical version of the SWIFT APIs) and (ii) the Partner then requests/calls on the SWIFT APIs; in all cases the appropriate credentials will be used when an End User accesses the integrated/embedded SWIFT Services.

A Partner enabling the Business Connect Solution to End Users will necessarily use the Business Application Model for such purpose.

The Enabler Programme is intended to enhance or provide complementary value to the Partner's Partner Service offering, as well as ease the technical effort for the End User to implement, configure and use SWIFT Services and is not intended to be simply an opportunity to act as a reseller of SWIFT Services.

INTRODUCTION

Partner is subject to the specific terms and conditions as described in these "**Enabler Terms and Conditions".** These Enabler Terms and Conditions (including the Annexes hereto) taken together with the Partner Schedule and any relevant SWIFT Quotations related to the Programme and associated with e-orders accepted by SWIFT are referred to as the "**Agreement"**. The Agreement, as it relates to a particular Partner, may be modified or terminated, without prejudice to any other Agreement between SWIFT and any other Partner.

1. ELIGIBILITY AND PARTNER WARRANTIES

1.1 While SWIFT reserves the right to determine in its absolute discretion which Partners will be admitted to participate in the Programme, as a general matter SWIFT may consider, among other things, whether (i) a Partner's application or solution or middleware being integrated with the relevant SWIFT Services could be considered complementary or ancillary to such SWIFT Services and (ii) distribution and consumption of such SWIFT Services through the Partner's application or solution or middleware will appeal to a significant number of SWIFT customers, bring significant value to the SWIFT community and be consistent with SWIFT's business objectives.

1.2 Partner is required to register as a registered provider under the SWIFT Partner Programme and comply with the additional obligations and requirements as described therein. Registration and compliance with the SWIFT Partner Programme must be maintained throughout the term of this Agreement. Failure to do so will automatically and immediately terminate this Agreement.

1.3 Partner must identify which Enabler Programme model (Business Application Model or API Concentrator Model) it will participate in and comply with applicable terms and obligations set out in the Enabler Terms and Conditions and the Agreement accordingly.

1.4 Partner may be required to maintain and comply with a certain level of security and operational requirements throughout the term of this Agreement, based on its selected model and the SWIFT Service(s) it enables. These requirements may vary depending upon (i) the operational deployment of the Partner Service, (ii) the particular SWIFT API that Partner has been authorised to distribute, (iii) whether Partner is enabling the Business Connect Solution and/or (iv) any additional SWIFT Programmes in which the Partner currently participates. Those requirements that must be met at all times are referenced in **Annex 1** (Security and Operational Requirements). Furthermore, Partner will necessarily be required to meet and comply with the requirements referenced or set out in **Annex 2** (Partner Accreditation Process). Certain terms and requirements that pertain to a Partner that is authorised to enable connectivity to the SWIFT messaging network through the Business Connect Solution are set out in **Annex 7** (Service Enablement of Business Connect Solution) and as to such Partner, when acting in such capacity, the terms of **Annex 7** apply; to the fullest extent possible, the terms of **Annex 7** shall be considered in addition to, and cumulative with, the terms set out elsewhere in the Agreement, provided that the terms of **Annex 7** will take precedence over any terms set out elsewhere in the Agreement, to the extent such terms are in conflict with the terms of **Annex 7** and cannot reasonably be cumulated with the terms set out elsewhere in the Agreement. Partner's failure to meet and maintain compliance with any of these requirements entitles SWIFT to (at its sole discretion) immediately terminate this Agreement.

1.5 Partner warrants that:

a. it will always integrate/embed the SWIFT Services with one or more of its Partner Services using a Business Application Model or API Concentrator Model, maintaining full transparency of each End User using the Partner Service and keeping data appropriately separated for each respective End User; it will not promote or offer any SWIFT Service as a standalone service to End Users (that is, it, will not resell such service as a non-integrated/non-embedded service);

b. any use of SWIFT Services, and/or any use of components such as SWIFT SDK or SWIFT Microgateway or SWIFT API Gateway or Alliance Cloud, will be done in accordance with the relevant service description and SWIFT contractual documentation;

c. its entering into, and its performance of, this Agreement has been duly authorised, and that performance of this Agreement does not and will not conflict with any provision of any of its corporate governance documents or any law or regulation or material obligation by which it is bound.

2. RIGHTS GRANTED TO THE PARTNER

2.1 SWIFT grants Partner a non-exclusive, personal and non-transferable right:

a. to distribute the SWIFT Services, in accordance with the terms and conditions of this Agreement.

b. to the extent that Partner is enabling, SWIFT Services through SWIFT APIs, (i) request/call on the SWIFT APIs for the sole purpose of delivering the SWIFT Services in a functional, effective and uncorrupted form to End Users and (ii) pass on (or cause to be passed on) identical and uncorrupted copies of the SWIFT APIs to the End User and/or the relevant Distribution Element; provided that each End User and Distribution Element is and at all times remains adequately identified to SWIFT.

2.2 The right granted under article 2.1 is limited to the duration of this Agreement and subject to all of the following:

a. SWIFT confirming in writing to the Partner that the Partner has qualified for the Enabler Programme per **Annex 2** (Partner Accreditation Process) with respect to each relevant SWIFT Service;

b. acceptance and continuing subscription (in a manner satisfactory to SWIFT) by the End Users of (i) SWIFT's standard service terms for the applicable SWIFT Service and (ii) the end user policy ("**End User Policy**") for the Enabler Programme (containing important information and terms for the End User obtaining SWIFT Services through a Partner) that is referenced in **Annex 3** hereto. Upon first request of SWIFT, Partner must provide SWIFT with evidence of such acceptance and subscription. SWIFT may deny the relevant End User access to the SWIFT Services (or, if access was already granted, SWIFT may revoke such access) if such acceptance and subscription cannot be evidenced; and

c. compliance by Partner with the relevant SWIFT Services terms and conditions applicable to the SWIFT Services, particularly with regard to their application to Partners involved in distribution of, or playing a functional/operational role with respect to, such SWIFT Services; for ease of reference, **Annex 4** (SWIFT Services and Related Terms) references the SWIFT Services terms and conditions, including, but not limited, to the SWIFT Software Development Kit (SDK) Service Description and the SWIFT Microgateway Service Description and the SWIFT API Gateway Service Description (such service descriptions are collectively referred to as the "**API Service Descriptions**"), which relate to accessing SWIFT Services through SWIFT APIs.

d. Partner understands and agrees that the consumption of SWIFT Services is limited to SWIFT customers that are End Users and Partner is not entitled or permitted to consume any SWIFT Services for itself. Further, Partner may not make use of any SWIFT Services, beyond what is contemplated in these Enabler Terms and Conditions in connection with fulfilling Partner's role in the distribution of such SWIFT Services to End Users.

3. PARTNER'S ROLE AND RESPONSIBILITIES

3.1 Partner is responsible for ensuring that its enabling of the SWIFT Services as contemplated by this Agreement (the "**Service Enablement**") is permitted under applicable law. Partner undertakes to monitor any change in applicable law and to amend its Service Enablement in case it is required to comply with a change in applicable law. In the event that any such amendment would result in breach of the terms of this Agreement, such breach shall not be considered to be excused or waived by SWIFT.

If such amendment would not, in Partner's reasonable opinion, be practicable, Partner shall notify SWIFT of the change in applicable law and of the reason why it is not practicable to proceed to such amendment to comply with applicable law. If:

a. SWIFT agrees with Partner that it is not practicable for Partner to amend its Service Enablement, SWIFT shall terminate this Agreement under article 12.3;

b. SWIFT does not agree with Partner that it is not practicable for Partner to amend its Service Enablement of the SWIFT Services, SWIFT can terminate this Agreement under article 12.3 and the parties agree to submit this dispute to the dispute resolution mechanisms described under articles 15.5 to 15.7 of this Agreement.

3.2 Partner shall operate at all times in accordance with this Agreement (including its Annexes) but also within the spirit of the Partner Programme. Without prejudice to the generality of the foregoing, Partner undertakes in particular to:

a. conduct its business in a way that does not adversely affect SWIFT's interests or business, products or services, security, goodwill, name, trademarks, or high reputation;

b. conduct itself with integrity, and act in accordance with the highest professional standards;

c. act in compliance with all applicable laws and regulations (including but not limited to anti-bribery, anti-corruption and anti-money laundering laws and regulations);

d. apply for, obtain and have renewed all permits, authorisations and licenses required for its activity at its own expense;

e. provide the End Users with accurate information about SWIFT, its services and products and, in particular, the SWIFT Services and, in the case of Partner providing any SWIFT Service through SWIFT APIs, the SWIFT APIs;

f. when operating in the API Concentrator Model, notify SWIFT at least 30 days prior to introducing or involving any additional or different Distribution Element or any material change to its Service Enablement and keep SWIFT apprised of all information SWIFT may reasonably request concerning any Distribution Element or aspect of the Service Enablement; SWIFT may terminate this Agreement should it reasonably determine that any aspect of a Partner's Service Enablement or any aspect of a Distribution Element is resulting in ongoing serious disruption of a SWIFT Service;

g. when operating in the API Concentrator Model, take all commercially reasonable steps to assure that any third party involved in the Partner's Service Enablement is acting within the scope of, and in a manner that is aligned, and not inconsistent, with the obligations of the Partner under this Agreement;

h. keep SWIFT apprised of all information regarding the Partner Service or any aspect of the Service Enablement (and/or any changes thereto) that could be expected to affect or impact the Service Enablement, as well as any other material changes to the Partner Service or the Business Application Model or API Concentrator Model described in the Partner Schedule;

i. take all appropriate precautions to keep the End User use of SWIFT Services and related data separated and exclusive to such End User, and notify SWIFT immediately if it becomes aware of inappropriate access of its End Users or inappropriate sharing of data from SWIFT Services between or among its End Users;

j. observe and comply with any terms of the SWIFT Services that may apply to Partner and follow any reasonable instructions of SWIFT in this regard or in connection with the Service Enablement or operational or security matters.

3.3 Partner shall comply at all times with:

a. The operational and security requirements referenced in **Annex 1** (Security and Operational Requirements);

b. The accreditation framework/process referenced in **Annex 2** (Partner Accreditation Process)

3.4 Partner holds the contractual relationship with SWIFT under this Agreement. However, SWIFT remains the direct contact towards End Users for all matters relating to the SWIFT Services and the SWIFT usership/membership; Partner understands and agrees that nothing in this Agreement restricts SWIFT's ability to enforce the terms of any contractual documentation between SWIFT and End Users or to admit or not admit a particular entity to become a SWIFT user or customer. Should SWIFT (or End User) terminate or suspend a SWIFT Service being used by an End User per the terms of relevant contractual documentation for such SWIFT Service, Partner will necessarily no longer be able to provide such service to such End User through Partner's Service Enablement.

3.5 Partner is responsible for accessing the latest information made available by SWIFT in connection with the performance of this Agreement. Partner shall regularly, or promptly upon SWIFT's prior written notice, consult the latest available information (typically on www.swift.com).

4. SWIFT'S ROLE AND RESPONSIBILITIES

4.1 SWIFT shall give Partner such access to information, marketing documentation and other materials as is reasonably necessary for the performance of this Agreement.

4.2 SWIFT agrees to give visibility to Partner and its Partner Service and qualification with respect to its Service Enablement of the SWIFT Services through SWIFT's official website: www.swift.com. SWIFT reserves the right to remove Partner's name and/or any such status in the event of non-compliance by Partner with the applicable requirements and criteria set out in this Agreement.

5. FEES

5.1 SWIFT will invoice Partner for the rights granted under articles 2.1 and 9.2, and Partner will timely pay SWIFT the fees specified or referenced in, and otherwise comply with, **Annex 5** (Fees/Financial Conditions).

5.2 Except as may be otherwise provided in the Agreement, SWIFT's Pricing and Invoicing – Ordering, Invoicing and Payment document applies to invoicing and payment. Partner will pay SWIFT by direct debit (unless otherwise notified by SWIFT).

5.3 Each party will otherwise pay its own costs incurred in connection with the performance of this Agreement.

6. CO-OPERATION

6.1 Each party shall assign a coordinator for the performance of this Agreement and shall promptly notify the other party if the coordinator changes.

6.2 Each party shall provide to the other party the contact details of the coordinator no later than on the date that this Agreement commences (and shall promptly communicate any changes to such contact details). Partner shall set forth such contact details in the Partner Schedule.

6.3 The parties agree to use all reasonable efforts to give regular feedback on the performance and execution of this Agreement.

7. COMMUNICATION

7.1 Each party acknowledges and agrees that the other party may disclose or advertise the existence of this Agreement between them to any interested prospects or other third parties.

7.2 Any campaign, announcement, website content, press release, advertising or marketing collateral or similar publicity of Partner that in any way relates or refers to the Enabler Programme or the matters contemplated hereby or that refers to the SWIFT Services or Partner Service (as it relates to the Service Enablement) must first be approved in writing by SWIFT. As such, SWIFT desires to ensure consistent naming and branding of its solution in all communications.

8. SUPPORT

8.1 Partner must promptly inform SWIFT when:

a. the Partner Service or the Business Application Model or the API Concentrator Model (or any relevant Distribution Element) is disrupted or otherwise subject to security or operational issues that could reasonably be expected to impact the SWIFT Services; and

b. any SWIFT Services within or paired with the Partner Service is disrupted or otherwise subject to security or operational issues that could reasonably be expected to impact the SWIFT Services, in which case Partner also undertakes to provide all assistance and information to assist SWIFT in dealing with such disruption or issues or answering any queries from End Users relating to such disruption or issues.

8.2 Any support provided by SWIFT in relation to the Service Enablement is covered in the API Service Descriptions or, in the case of enablement of the Business Connect Solution, in the Alliance Cloud Service Description and will be at the level of SWIFT Community Support (unless otherwise agreed by SWIFT). This support is conditioned upon the SWIFT Service being included in the accreditation process and being a SWIFT Service for which the Partner is authorised to distribute per the Enabler Programme and the Agreement.

The Partner understands that:

- It is responsible for the ongoing operation of its Partner Service, which has SWIFT API functionality embedded, and the Service Enablement and the Partner should direct its End Users to contact the Partner in the instance any disruption to the Partner Service or Service Enablement.

- If an operational issue arises which is investigated because of an apparent issue with the SWIFT API service or the Business Connect Solution, as the case may be, the Partner should raise a case with SWIFT Support through the appropriate channels in order to help SWIFT resolve the issue and identify impacted End Users.

8.3 SWIFT requires that the Partner define a service level agreement (SLA) with its End Users in terms of providing a response when a support case is raised, and likewise that Partner defines an SLA to respond to SWIFT when actively resolving End User support cases.

9. INTELLECTUAL PROPERTY RIGHTS

9.1 Each party owns, and will continue to own all right, title and interest in and to any material, software, information, trade secrets, materials, property that it owned prior to this Agreement, or that it independently created or acquired pursuant to this Agreement. In particular, any and all rights, including title, ownership rights, goodwill, copyright, trademarks, patents, and any other intellectual property rights of whatever nature (together, the "**Intellectual Property Rights"**), in the information, documentation and other materials made available by one party to the other in connection with this Agreement will remain the sole and exclusive property of such party or its licensors. For the avoidance of doubt, this means that SWIFT will retain all right, title and interest (as described in this article 9.1) in the SWIFT Services and the Business Connect Solution, SWIFT SDK, SWIFT Microgateway, SWIFT API Gateway and SWIFT APIs and that to the extent permitted under applicable law, Partner undertakes not to modify, reverse engineer, decompile, or disassemble any aspect of any of the SWIFT Services, Business Connect Solution, SWIFT SDK, SWIFT Microgateway, SWIFT API Gateway or SWIFT APIs.

9.2 As indicated under article 2.1, Partner is granted a non-exclusive, personal and non-transferable right to enable distribution of the SWIFT Services per the Service Enablement in accordance with the terms

and conditions of this Agreement. In particular, SWIFT grants Partner a non-exclusive, personal and non-transferable right to use information, documentation and other materials made available by or for SWIFT to Partner in connection with this Agreement as necessary for the performance of its obligations under this Agreement. Any such use must conform to any instructions or guidelines given by SWIFT to Partner. Unless expressly provided otherwise, Partner is not allowed to translate or modify such title, information, documentation or other materials, and may not embed, merge or otherwise integrate them into any other documentation or materials without the prior written approval of SWIFT.

9.3 Without prejudice to article 9.1, SWIFT may request from Partner a licence to use Partner's Intellectual Property Rights to the extent that such Intellectual Property Rights may be useful to improve the SWIFT Services. Partner shall not unreasonably refuse such request. In case Partner grants a licence to SWIFT under this article 9.3, the parties shall agree on the terms of such licence in a separate agreement.

9.4 Partner grants SWIFT a non-exclusive, personal and non-transferable right to use the information, software and other materials made available to SWIFT by or for Partner for the purpose of executing its rights and obligations under this Agreement. Such information and materials may include Partner's name and logo.

9.5 Partner must use SWIFT trademarks according to the SWIFT Trademark Guidelines available on www.swift.com > About SWIFT > Legal > SWIFT Trademark Guidelines.

10. CONFIDENTIALITY

10.1 Each party can use confidential information of the other party only for the purposes of exercising its rights or for performing its obligations in connection with this Agreement.

10.2 Each party will keep confidential and not disclose the terms of this Agreement and other information, documentation and materials made available by or for the other party in connection with this Agreement, all in accordance with the non-disclosure agreement set out in Annex 6. Notwithstanding anything to the contrary in this Agreement, SWIFT may make these Enabler Terms and Conditions and Annexes public on its website.

Notwithstanding any term to the contrary in this Agreement, SWIFT reserves the right to share with End Users confidential information (i) to the extent contemplated by, or necessary to perform, this Agreement; and (ii) in exceptional cases and on a need-to-know basis only for the purposes relating to the provision, security (including forensic investigations) or support of Partner Service and/or SWIFT Services provided in connection with this Agreement. For the avoidance of doubt, Partner acknowledges and agrees that SWIFT may share information regarding Partner (such as the name, Partner Identification Code [PIC] or other identification code and qualification status). Furthermore, SWIFT may share confidential information to the extent, and under conditions, consistent with the confidentiality obligations set out in the SWIFT General Terms and Conditions.

10.3 For the purposes of any on-site inspections or audits with respect to the compliance by Partner with this Agreement, all SWIFT-appointed (third-party) auditors are bound by a confidentiality undertaking or obligations of confidence which are no less stringent than those that apply to SWIFT hereunder.

11. LIABILITY

11.1 Subject to the limitations set forth below, each party shall be responsible and liable vis-à-vis the other for any and all damages, losses, injury, expenses or liabilities of whatever nature, arising out of any negligence in the performance of its obligations or any breach of its any of its obligations, representations or warranties set forth in this Agreement.

11.2 SWIFT is not liable to Partner for damage caused by the SWIFT Services except to the extent that such damage is solely and directly caused by the SWIFT Services.

11.3 In no event shall either party be liable to the other for any indirect, incidental, special, exemplary or consequential damages, including but not limited to loss of business or profit or revenue, even if the party has been advised of their possibility. Except as otherwise expressly provided herein, each party's exclusive remedy for claims related to the execution of this Agreement is limited to proven direct damages caused by the other party's fault and in an aggregate maximum and cumulative amount not to exceed the greater of (1) 10,000 Euro** or (2) the aggregate amount of fees paid by the claiming party to the other in connection with the Enabler Programme and/or this Agreement in the 12 months immediately preceding the initial event giving rise to any such claim. These limitations of liability do not apply in the case of (i) claims for fees and amounts required to be paid pursuant to the express provisions of this Agreement or (ii) the indemnification obligations of Partner set out in article 11.4, nor in the case of fraud or wilful misconduct. To be valid, a party must notify the other of its intention to file a claim no later than 3 months after becoming aware of the damaging event.

**see Annex 7 for monetary cap relating to Business Connect Solution

11.4 Partner is liable towards End Users for the provision of the Partner Service and for the Service Enablement. Nothing in the contractual framework with End Users can be understood as a waiver of its responsibility, in particular with respect to compliance with security, confidentiality, data handling and integrity obligations arising per this Agreement. Partner shall indemnify, defend and hold SWIFT and its directors, affiliates, employees and representatives (collectively, the "**SWIFT Parties"**) harmless from and against any and all third-party (including End Users) and other claims and related losses, liabilities, damages, costs and expenses (including, but not limited to, reasonable attorneys' fees) received or incurred by any of the SWIFT Parties arising out of or related to (i) the Partner Service or the Service Enablement, and/or (ii) a breach by Partner of any obligation, representation or warranty, set forth in this Agreement and/or any related SWIFT contractual documentation, in particular any security or operational requirements imposed on Partner.

11.5 For the sake of clarity, the parties' liability with respect to the provision and use of the Business Connect Solution, SWIFT SDK, SWIFT Microgateway, SWIFT API Gateway, SWIFT APIs and any other SWIFT Services or products shall be subject to the respective term and conditions and relevant service descriptions, as may be applicable to those services and products (including liability limitations set out in such contractual documentation).

12. TERM AND TERMINATION

12.1 This Agreement shall be of indefinite term, subject to termination as provided herein.

12.2 In case of breach by either party of its obligations under this Agreement, the other party shall be entitled to terminate this Agreement, in whole or in part, at any time immediately upon notice to the other party (and without court intervention) if such breach is material and (i) is incapable of remedy or (ii) has not been remedied within thirty (30) calendar days after notice of such breach shall have been given to the party in breach by the other party.

12.3 To the extent not contrary to mandatory law, the following situations shall be considered as exceptional circumstances (default situations) that justify the early termination of this Agreement by the non-defaulting party at any time immediately upon notice to the other party (and without court intervention):

a. Discontinuation by SWIFT of any or all of the SWIFT Services (it being understood that SWIFT may, at its sole discretion, put in place a migration plan) where an affected Partner terminates the Agreement;

b. Bankruptcy, insolvency, moratorium, receivership, liquidation or any kind of composition between a party and its creditors, or any circumstances likely to affect substantially one party's ability to carry out its obligations under this Agreement;

c. Change of control or ownership of Partner;

d. Loss by Partner of its SWIFT Partner status for whatsoever reason (including where not caused by a breach of this Agreement);

e. A party becoming subject to sanctions or export control laws or regulations that restrict the other party from dealing or doing business with such party or any Distribution Element or third party associated with a Distribution Element as contemplated hereby;

f. A situation described under articles 1.2, 1.3, 1.4, 3.1 or 3.2(f) where SWIFT terminates the Agreement.

12.4 Either party may terminate this Agreement for convenience by giving the other party at least three (3) months' prior written notice of termination.

In the event of such notice of termination: (A) SWIFT may (i) remove references to the Partner and/or its Partner Service and/or its Service Enablement and/or related qualifications from that part of SWIFT's website intended to give visibility to Partner's participation in the Enabler Programme and (ii) cease to provide any commercial/marketing support for the Partner, or identification of the Partner, with regard to its participation in the Enabler Programme and, unless otherwise agreed by SWIFT, any right granted to the Partner to use branding or materials associating Partner with the Enabler Programme shall cease; and (B) the Partner shall not bring on any new or additional End User to the Enabler Programme, shall not make any new/additional SWIFT Services available to any existing End User, and shall cease to use any branding, collateral, materials or other publication or publicity associating the Partner with the Enabler Programme.

12.5 In the event of termination of this Agreement, SWIFT shall not be responsible for migration costs associated with moving End Users to direct service provision by SWIFT or any other entity with regard to SWIFT Services.

12.6 The termination of this Agreement for whatever reason does not release Partner of any of its obligations arising prior thereto or which expressly or by implication become effective or continue to be effective after such termination, such as obligations regarding confidentiality or liability.

12.7 In the event that SWIFT has made available more than one SWIFT Service for Service Enablement by a Partner, SWIFT reserves the right, when exercising any termination right set out in this article 12, to terminate this Agreement partially and only as to any one or more of the Service Enablement(s) for such SWIFT Service(s). In such instance, the terms of this article 12 shall apply, *mutatis mutandis*, to the termination of Partner's Service Enablement with respect to the SWIFT Service(s) in question.

12.8 In certain specific instances of non-compliance by Partner with its obligations, SWIFT reserves the right to invoke an escalation process as may be set out in the terms of Annex 1 and/or Annex 2. Instituting such an escalation process cannot be considered to be a waiver by SWIFT of any of the contractual provisions or remedies described in this article 12 or elsewhere in these Enabler Terms and Conditions.

12.9 To the extent that it is authorised under applicable law, the following articles will survive the termination or expiration of this Agreement for an indefinite period of time: 3, 5, 7.2, 9, 10, 11, 14, and 15.

13. **DATA PROTECTION**

13.1 As used in this article 13.1, “Controller”, “Data Subject”, “Personal Data” and “Processing” shall have the meaning given to these terms in the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) as amended and replaced from time to time (hereinafter referred to as “EU Data Protection Law”). Each party acknowledges and agrees that the other party may Process Personal Data related to its staff (“Staff data”) as a Controller for the party’s own purposes relating to security and fraud detection, accounting and record keeping, and more generally, the performance of its own obligations under this Agreement. Each party will Process Staff data in accordance with all applicable privacy, data protection and information security laws, including EU Data Protection Law where relevant. Each party acknowledges (and shall cause its Staff concerned to acknowledge) that each member of the Staff can exercise its Data Subject rights by sending a written request together with a proof of identity to the other party: to SWIFT’s Privacy Officer at privacy.officer@swift.com for Staff of the Partner and to the Partner’s address set forth in its Partner Schedule for SWIFT Staff.

Each party will take all appropriate technical and organisational measures to protect Personal Data against accidental or unauthorised destruction, accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing. Each party acknowledges that the Personal Data may not be kept indefinitely or longer than needed for the intended Processing.

14. NOTICES

14.1 Any notice required or formulated hereunder may be personally delivered or sent by courier or registered mail or e-mail to the following addresses for notices, which may be updated from time to time by one party giving written notice of such update to the other:

a. Notice to SWIFT:
SWIFT SC
Avenue Adéle
B – 1310 La Hulpe
Belgium

ATTENTION: Partner Management

E-mail: partner.management@swift.com

b. Notice to Partner:

Per the Partner Schedule

14.2 Any such notice shall be effective upon receipt.

15. MISCELLANEOUS

15.1 SWIFT and Partner are independent contractors and will have no power or authority to assume or create any obligation or responsibility on behalf of each other with regard to the performance of this Agreement or the Service Enablement or the SWIFT Services. This Agreement will not be construed to create or imply any structural partnership, agency, or joint venture.

This Agreement is the complete and exclusive agreement between SWIFT and Partner with respect to the subject matter hereof, and supersedes any other agreements or communications regarding the subject matter and may, except as otherwise provided in this article, only be modified, or any rights under it waived, by writing executed by authorised representatives of both SWIFT and Partner. Notwithstanding the preceding provisions of this article, SWIFT may unilaterally amend this Agreement (including any Partner Schedule) from time to time by posting the amendment or the amended terms on swift.com at least three (3) months’ prior to such amendment becoming effective

and/or by giving Partner at least three (3) months' prior notice of such amendment by e-mail or through other means permitted under this Agreement. In case of unilateral amendment of any Partner Schedule, SWIFT will provide prior notice of such amendment by e-mail or through other means permitted under this Agreement. In addition to and separate from any amendment procedure set out above, SWIFT may always unilaterally amend terms set out or referenced in Annexes to this Agreement to the extent stated in such Annexes and in the absence of any such stated amendment procedure, amendment may be made in the same manner as amendment of this Agreement. For avoidance of doubt, the SWIFT contractual documentation (including but not limited to the SWIFT General Terms and Conditions) and service descriptions (including but not limited to the API Service Descriptions) for SWIFT Services will be subject to the amendment procedures set forth or referenced therein or in the SWIFT General Terms and Conditions, as the case may be. SWIFT undertakes not to exercise the right to unilaterally amend this Agreement in an abusive manner and Partner may object to such unilateral amendment by exercising its termination right as provided under article 12.4.

15.2 Failure or delay to enforce any term of this Agreement shall not constitute a waiver hereof.

15.3 If any provision of this Agreement is found to be unenforceable, such provision will be enforced to the maximum extent permissible so as to approach as much as possible the intent of SWIFT and Partner, and the remainder of this Agreement will continue in full force and effect.

15.4 This Agreement will be governed by and construed in accordance with the laws of Belgium.

15.5 The parties will use all reasonable efforts to amicably resolve any issues that may arise between them in relation to this Agreement. They will escalate any such issues to their senior level of management, before attempting to solve their dispute according to any arbitration/litigation proceedings referenced in this article 15.

15.6 Any disputes not solved by mediation within three months upon a party's request to initiate mediation will be finally settled under the Rules of Arbitration of the International Chamber of Commerce then in force (the "**Rules**") before three arbitrators appointed in accordance with the Rules. Unless the parties agree otherwise, all proceedings are to be held in Brussels and in English and the award shall be based solely on documents and information provided in the English language, including where the original was written in a language other than English.

15.7 Notwithstanding the foregoing, SWIFT reserves the right to commence legal proceedings in relation to a claim against a Partner before the courts of the jurisdiction in which the Partner is established or conducts business.

15.8 Neither party shall assign or transfer any of its rights, or delegate any of its obligations, under this Agreement without the other party's prior written consent. In case Partner wishes to delegate or outsource or subcontract any obligation it may have or otherwise rely on another entity with respect to hosting or operating the software or hardware associated with the Partner Service and/or any SWIFT Services and/or Service Enablement, Partner shall first give reasonable prior notice to SWIFT of its intent to delegate, outsource or subcontract and the identity of the third party entity that will take care of the delegated, outsourced or subcontracted task, as well as any other relevant circumstances or particulars. SWIFT reserves the right to object to and prohibit such delegation, outsourcing or subcontracting, should it have a reasonable basis for doing so. SWIFT reserves the right to use subcontractors to carry out any on-site audits or inspections or any related activities, with SWIFT always remaining responsible for the performance by such subcontractors of such audits, inspections or activities.

15.9 In case of any conflict between the terms of this Agreement, its Annexes, the Partner Programme Terms and Conditions and the respective applicable SWIFT contractual documentation and service descriptions, the following order of priority shall apply:

a. this Agreement;

b. its Annexes;

c. the Partner Programme Terms and Conditions; and

d. the applicable SWIFT contractual documentation and service descriptions.

16. **AUDIT**

16.1 SWIFT reserves the right to assess continued compliance with this Agreement (and with any other contractual documents between SWIFT and Partner in relation to the Enabler Programme), by asking for supporting documents and/or information at any time during the term of the Agreement but also by consulting public sources, conducting onsite and/or remote inspections or audits, and/or collecting the End Users' feedback. The Partner acknowledges and agrees that SWIFT may require that the internal auditors of the Partner confirm, in writing, the accuracy and completeness of any information or data supplied by the Partner pursuant to this article 16.1.

16.2 Notwithstanding the preceding article 16.1, but subject to article 16.4, SWIFT will only require an on-site and/or remote inspection or audit if (i) there exist reasonable doubts about Partner's compliance with operational or security requirements or other material provisions of this Agreement, (ii) there is a significant reported security or operational incident that does not appear to have been timely and satisfactorily addressed by Partner or (iii) based on previous inspection or audit results or risk(s) identified by SWIFT, SWIFT continues to believe in good faith that Partner is not in compliance with its obligations under this Agreement. Whether an inspection or audit (or any portion thereof) will be conducted on-site or remotely will be at SWIFT's discretion.

16.3 SWIFT will use all reasonable efforts to perform any on-site or remote inspection/audit in a way that does not interfere with the Partner's normal business conduct. Subject to article 16.4 and the separate audit rights referred to in such article, charges for an inspection/audit are borne by SWIFT, unless the inspection/audit reveals non-compliance by Partner, in which case Partner shall promptly reimburse SWIFT for such charges.

16.4 In addition to the foregoing audit/inspection rights, please refer to the audit/inspection rights that are set out in **Annex 1** (Security and Operational Requirements). The audit/inspection rights in Annex 1 are separate from, and in addition to, the foregoing audit/inspection rights. Nothing in the preceding sections of this article will modify or affect the audit/inspection rights in **Annex 1.**

ANNEXES:

- Annex 1: Security and Operational Requirements
- Annex 2: Partner Accreditation Process
- Annex 3: End User Policy
- Annex 4: SWIFT Services and Related Terms
- Annex 5: Fees/Financial Conditions
- Annex 6: Mutual NDA
- Annex 7: Service Enablement of Business Connect Solution

ANNEX 1

Security and Operational Requirements

SWIFT reserves the right, to amend/update from time to time, typically yearly, the Security and Operational Requirements upon reasonable prior notice to Partner (including notice by either e-mail and/or by posting a new version on www.swift.com).

1. Release Timeline updates

Partners utilizing APIs to enable SWIFT Services must diligently follow the SWIFT Release Timeline, as made available on www.swift.com, in addition to the relevant Release Notes for components such as SWIFT API Gateway, SWIFT SDK and/or SWIFT Microgateway, and material made available on the SWIFT Developer Portal in relation to new versions of SWIFT APIs.

All Partners are expected to undertake the necessary updates as they relate to SWIFT Services and/or SWIFT APIs to ensure the Partner Service is capable to execute the continuous delivery of Service Enablement, as new API versions or product versions or service descriptions are released and older versions are deprecated.

When deploying security or functional updates, the Partner should notify End Users as to the importance and urgency to install/implement such updates, as appropriate.

The Partner must assure that its solution or application or middleware is duly adapted and revised to integrate/embed the appropriate release versions of SWIFT APIs and components such as the SWIFT API Gateway, SWIFT SDK and/or Microgateway (where applicable - as made available on the SWIFT Developer Portal) and is also properly aligned with any operational requirements and modifications as part of the current version(s) of the SWIFT Service which it is embedding/integrating.

More details about the upgrade schedule of the SWIFT API Gateway, SWIFT SDK and/or SWIFT Microgateway can be found in the relevant Service Descriptions as made available on swift.com.

2. Compliance with the Provider Security Controls Framework (PSCF)

SWIFT defines specific requirements as they relate to the security and resilience of the Partner Service and relevant aspects of Partner's operational infrastructure in a document known as the Provider Security Controls Framework (PSCF) which is made available in the Knowledge Centre on swift.com.

The Provider Security Controls Framework document establishes a set of mandatory operational and security controls for the operating environment of entities in the Enabler Programme and/or providing shared connectivity to the SWIFT network to SWIFT users. The controls detailed are product agnostic and are benchmark conditions to be adhered to, they should not be considered to replace a well-structured security and risk framework. The controls defined for Partners in the Enabler Programme are separate from, and do not supersede nor replace, any other applicable requirements from other SWIFT Programmes in which the Partner may participate (for example, the Shared Infrastructure Programme or Lite2 for Business Applications Programme).

All Partners must comply with the Provider Security Controls Framework. There are several possible operational configurations of the infrastructure for a Partner participating to the Enabler Programme. Based on the infrastructure and the involvement of SWIFT's network (MVSIPN), the Partners are categorized as "**Enabler Type 1**" or "**Enabler Type 2**" which define the assessment method as explained below. Partners providing the Business Connect Solution will be in the Enabler Type 2 category.
In this document, Partners in the Enabler Programme are sometimes referred to as "**Enablers**" or "**Solution Providers**".

2.1 Assessment method by Enabler type:

The assessment method of the compliance against the Security and Operational requirements as defined in the Provider Security Controls Framework document depends on the Enabler Type:

- The Enablers Type 1 are assessed through:
  - an annual self-attestation
- The Enablers Type 2 (including Enablers supporting the Business Connect Solution) are assessed through all of the following methods:
  - an annual self-attestation
  - on-site or remote inspection at the Solution Provider
  - continued remote verification

SWIFT will inform the Enabler of its Enabler Type. Enabler Type may change due to Enabler's offering new or different SWIFT Services or pursuant to changes to the Security and Operational requirements that apply to the Enabler Programme.

2.2 Annual Self-Attestation

Scope

On an annual basis, all Solution Providers have to self-attest full compliance against all Security and Operational requirements by the end of that year. In case, for an Enabler Type 2 Solution Provider, an on-site inspection (parts or all of which may be conducted remotely) is planned in the same year, it is not required to submit clarifications and potentially a new self-attestation for such year. New Solution Providers are requested to send their self-attestation compliance within 1 month after activation of live service.

Data collection

The self-attestation will have to be done by means of filling out the required attestation templates in paper or electronic form, as will be indicated by SWIFT. The reference control set that must be self-attested against will be the version of the Security and Operational requirements as defined in the document Provider Security Controls Framework document that is applicable at that time.

Assessment

A positive evaluation by SWIFT of the self-attestation that shows compliance as per provided guidelines or equivalent alternatives (to the extent such alternatives are acceptable to SWIFT) on all requirements will lead to the Solution Provider being qualified against this latest control set and listed as such on the appropriate swift.com Directory. A positive evaluation will not be possible if observations would arise or remain from an onsite inspection. In case of doubts in the content of the self-attestation (incompleteness, lack of clarity, deviation from real status), SWIFT may request the Solution Provider to submit a new self-attestation. Failure to obtain a positive evaluation by the time indicated by SWIFT may start the escalation process as described in section 4 below.

2.3 On-Site Inspection

Scope

For all Solution Providers in the Enabler Type 2 category, an on-site inspection will be performed by SWIFT or SWIFT-appointed (third-party) auditors. **Whenever in this document an "on-site" inspection or audit is referred to, it is understood that parts or all of such inspection/audit may, at SWIFT's discretion,**

be conducted remotely. In case third-party auditors would be performing the inspections, they are held to the same confidentiality requirements as existing between the Enabler Type 2 Solution Provider and SWIFT. The frequency of the on-site inspections will depend on the risk classification of an Enabler Type 2 Solution Provider and will be no less than once every 3 years. SWIFT will use its best efforts to provide a planning for the calendar year by end of November of the preceding year. SWIFT reserves the right to perform an inspection at short notice in case it deems it warranted (for example in case of alleged security incidents or negative reports from users). SWIFT reserves the right to charge the standard rate of one consultancy day and any proven incurred costs in the following cases:

- A Solution Provider cancels its inspection less than 6 weeks in advance without any approved justification.
- SWIFT has to cancel the inspection because the requested data could not be delivered at the latest 2 weeks before the scheduled date of inspection.

Data Collection

At least one month before an on-site inspection is scheduled, the Enabler Type 2 Solution Provider will be asked to complete an audit survey and to deliver supporting documentation through a secure data exchange mechanism. Enabler Type 2 Solution Providers are requested to collaborate and provide information during the on-site inspection to complete any information that may have been missing during the remote verification. If the original information or document is not in English, the Solution Provider is requested to provide, in addition to the original information or document, an English translation of the information or document.

Assessment

A remote pre-assessment will determine whether an inspection can take place, depending on the quality of the requested information and the outcome of the controls that have been assessed upfront. At the end of the inspection, an exit meeting is organised to explain any observations made. The list of observations is shared with the Enabler Type 2 Solution Provider and enables them already to initiate the required remediation.

After the on-site inspection, the SWIFT-appointed (third-party) auditors document the observations presented during the exit meeting and when documented, submit the observations for management comments and to confirm a target closure date. The Solution Provider has 2 weeks to submit feedback on the observations. A final inspection report is issued 1 week after receipt of all Solution Provider comments. The final report includes the Solution Provider management comments and a rating. The rating will depend on the importance of the different controls and the severity of the noncompliance. This objective scoring will be an important factor in reaching one of the below compliance statuses:

- **Substantially meets requirements, with noted deviations (if any) having no/minimal negative impact**
  Most internal controls and processes inspected are operating effectively and substantially comply with the Security and Operational Requirements. Taken together or individually, any issues identified has no or only a minimal negative impact on the inspected Solution Provider and its capacity to provide service as defined in the Security and Operational Requirements.

- **Partially meets requirements, with noted deviations having considerable negative impact**
  A considerable portion of the inspected internal controls and processes need improvement to be fully effective and to comply with the Security and Operational Requirements. Taken together or individually, issues identified have had or could have a considerable negative impact on the inspected Solution Provider and impair its ability to fully meet its capacity to provide service as defined in the Provider Security Controls Framework document.

- **Substantial deviations from the requirements noted, with widespread significant negative impact**

Reviewed internal controls and processes are largely ineffective and substantially deviate from the Security and Operational requirements. Issues identified during the review would require immediate Management attention to ensure the capacity of the Solution Provider for providing service as defined in the Provider Security Controls Framework document. If the issue is considered as blocking, then SWIFT may trigger the escalation process within 1 month after the issuance of the final report. Blocking observations are full failures of security controls that already existed in relevant product/service releases and/or were raised as an observation during the previous on-site inspection.

Final report distribution

The Solution Provider may request SWIFT to distribute the final report to a third party (for example, existing and potential customers of the Solution Provider). The Solution Provider is not authorised to distribute the report directly. SWIFT reserves the right to use the final report internally for security purposes.

Usage of alternative certifications

A Solution Provider may provide evidence of capabilities by means of an ISAE 3000 report, ISO 27000 certification, or similar. Based on the type of documentation provided, as well as the scope of the activities covered in such a report, these reports will supplement and/or partly replace SWIFT's compliance assessment of the security and operational requirements as listed in the Provider Security Controls Framework document. The degree to which these reports will supplement and/or partly replace such assessment is in the discretion of SWIFT.

2.4 Continued Remote Verification

Scope

At random intervals, SWIFT may verify compliance to specific security and operational requirements.

Data collection

These checks can be done by requesting the Solution Provider to run diagnostic scripts and upload the output through remote verification by SWIFT on its own systems.

Assessment

Given the nature and criticality of the controls, all results must show compliance or an agreed short-term correction plan.

3. Renewal

Introduction

SWIFT reserves the right to assess continued compliance with the Security and Operational Requirements and any related contractual documentation by on-site inspection at least every 3 years, and in addition, by asking for supporting documents or information at any time during the term of the Solution Provider's participation in the Programme as previously mentioned in this Annex and in article 16 (Audit) of the Enabler Programme Terms and Conditions.

The applicable compliance criteria will be those established in the Enabler Programme Terms and Conditions at the time of the on-site inspection.

3.1 Overview of renewal conditions

A renewal is subject to:

- A new legal and financial due diligence process to check the continued adherence with legal and financial eligibility requirements.
- A new on-site inspection assessing the compliance with the Security and Operational Requirements as set out in the Provider Security Controls Framework.
- A yearly renewal of the used technology solution(s).

Note: The qualification criteria for a business segment may change from year to year to reflect market evolution and End User needs. In case of criteria changes, SWIFT may require re-validation. In selective cases, only technical validation is required for renewal. SWIFT maintains discretion to mandate re-qualification of the Solution Provider's Business Application Model or API Concentrator Model ensuing a major release change to the software as set out in Annex 2 (Partner Accreditation Process).

3.2 On-site inspection

SWIFT may request a new on-site inspection if, within this 3-year period, (i) SWIFT criteria have significantly changed (changes of criteria that impact operational reliability or security (for example, confidentiality, integrity, and availability) are considered as significant changes), (ii) in case of reported security or operational incidents, (iii) based on previous on-site inspection results or risk(s) profile identified or (iv) there exist reasonable doubts about Solution Provider's compliance with operational or security requirements as mentioned in article 16 (Audit) of the Enabler Programme Terms and Conditions.

On-site inspections performed in the context of assessing compliance with the Security and Operational Requirements are always at the expense of the Solution Provider. The costs and expenses are referenced in Annex 5 (Fees/Financial Conditions).

3.3 Consequences of a renewal failure

A failure to comply with these renewal requirements has the following consequences:

Qualification as a Solution Provider under the Enabler Programme is removed and escalation process described in next section is triggered.

4. Escalation process:

In case of non-compliance with the qualification conditions, including non-compliance with Security and Operational requirements as set out in the Provider Security Controls Framework identified by SWIFT after an on-site inspection, a self-attestation or additional tests being performed to ensure continued compliance, the escalation process is invoked as follows:

- **Step 1: Removal from the Enabler Programme Solution Providers SWIFT directory ("de-listing")**

  The de-listing occurs when the Solution Provider is not compliant with eligibility criteria and the requirements outlined in this Annex. The delisting has no impact on the continuity of the Solution

Provider operation. This step typically is invoked if observations from inspections or self-attestations are not proven remedied 6 months after an inspection report is issued or a self-attestation was submitted.

- **Step 2: Suspension**

This step is triggered by either of the following cases:

- Continued non-compliance 3 months after the de-listing from the Enabler Programme Directory with no commitment from the Solution Provider to remediate in the short-term. This means the Solution Provider will be prohibited from registering additional customers/end-users or providing any additional SWIFT services or products to End Users, as long as the non-compliance continues.

- Non-compliance 9 months after an initial inspection of a new Solution Provider that has never been listed in the Enabler Programme Directory. This means the Solution Provider will be prohibited from registering additional customers/end-users or providing any additional SWIFT services or products to End Users, as long as the non-compliance continues.

SWIFT reserves the right to notify the existing Solution Provider customers/end-users that their Solution Provider is suspended from the Enabler Programme because of continued non-compliance with the requirements.

- **Step 3: Termination**

This step is triggered in case of continued non-compliance 3 months after the suspension with no commitment from the Solution Provider to remediate in the short-term. In addition to the actions taken in Step 1 and Step 2, termination has the following consequences for the Solution Provider:

- Termination of all granted licences, such as licences for the User Handbook
- Termination of all access rights, such as access to support services and online ordering
- Revocation of the right to use certificates and titles
- De-activation of the partner identifier and BCPX code allocated to the Solution Provider
- Obligation for the Solution Provider to, at SWIFT's request, destroy or return those SWIFT services and products which are still in its possession
- In case of insolvency, bankruptcy, liquidation and other similar circumstances of a Solution Provider, the termination of the Solution Provider from the Programme takes place with immediate effect.
- Solution Provider will coordinate with SWIFT and find an alternative solution for the End Users during the transition (3 months from the day they have been notified by the Solution Provider or SWIFT, as the case may be)
- In the case of termination (either SWIFT or the Solution Provider) of its participation in the Programme, SWIFT will promptly notify each of its serviced End Users

Termination for Serious Non-Compliance

Nothing set out in this Annex or elsewhere in this Agreement shall prejudice SWIFT’s rights to terminate the Agreement for serious non-compliance with Security and Operational Requirements, or as may be otherwise permitted under the Enabler Programme Terms and Conditions of which this Annex is a part.

SWIFT reserves the right to communicate the status of the Solution Provider at its own discretion and at any stage of the escalation process to End Users and relevant regulatory authorities/supervisors.

5. Handling of Individual End Users of Solution Provider

Solution Provider must assist serviced SWIFT end users during the transition

In the case of termination (either by SWIFT or by the Solution Provider) of its participation in the Programme, the Solution Provider agrees to take the following measures:

- promptly notify each of its serviced End Users thereof
- enable its serviced End Users to make alternative arrangements, offer, to the extent authorised under this programme or applicable laws, its serviced End Users to continue performing as their Solution Provider for a period of at least three months after such notification.

Solution Provider acknowledges and agrees that SWIFT reserves the right to contact the End Users impacted by the termination. After termination, SWIFT reserves the right to provide End Users with direct assistance to find an alternative way of connecting to the SWIFT messaging network and/or receiving SWIFT services or products that may have been provided to end users through the Solution Provider.

SWIFT reserves the right to charge the Solution Provider for any additional support costs caused by a lack of assistance to the serviced end user in transition.

Termination by the Solution Provider of a serviced end user

Before ceasing to act as a Solution Provider for an End User, the Solution Provider must demonstrate to SWIFT that it has notified the End User of such termination with 3 months' prior notice, and must ensure reasonable efforts to support the End Users in finding alternative connectivity to SWIFT and/or alternative provision of subscribed SWIFT services and products that may have been procured through the Solution Provider.

Termination by a serviced end user

If the End User notifies SWIFT of its intention to terminate its connectivity or its reception of any SWIFT service or product through the Solution Provider, then SWIFT informs the Solution Provider thereof prior to deactivating the End User’s connection and/or SWIFT service or product through the related Solution Provider.

Surviving obligations

More generally, termination of a Solution Provider’s participation in the Enabler Programme for whatever reason does not release the Solution Provider of any of its obligations arising prior thereto or which expressly or by implication become effective or continue to be effective after such termination, such as obligations regarding confidentiality or liability.

Please contact your SWIFT Account Manager to obtain further information regarding the Security and Operational Requirements.

Compliance with the foregoing, including all applicable Security and Operational Requirements, as in effect from time to time, is a requirement of the Agreement between SWIFT and each Partner.

ANNEX 2

Partner Accreditation Process

SWIFT reserves the right to amend/update, from time to time, the Partner Accreditation Process terms upon reasonable prior notice to Partner (including notice by either e-mail and/or by posting a new version on www.swift.com).

The SWIFT Enabler Programme requires all Partners to qualify through an accreditation process aimed at determining technical and functional suitability/capability as it relates to enabling SWIFT Services, as well as compliance with certain Legal, Financial and Business criteria.

For Partners enabling SWIFT Services through APIs the focus will be on technical and functional suitability/capability as it relates to using APIs to enable distribution of SWIFT Services to the SWIFT customer/End User (see the part of this document with heading (FOR PARTNERS ENABLING SERVICES THROUGH APIs). For Partners enabling SWIFT connectivity through the Business Connect Solution, please see the part of this document with the heading "FOR PARTNERS ENABLING CONNECTIVITY THROUGH BUSINESS CONNECT SOLUTION".

Whether Partner has satisfactorily achieved the required accreditation is within SWIFT's discretion and judgement.

LEGAL AND FINANCIAL COMPLIANCE CHECKS CRITERIA

In order for SWIFT to assess compliance of an applicant Partner with the legal and financial eligibility criteria described under Eligibility, SWIFT may consult information in public sources and asks the applicant to provide corporate documentation, including but not limited to:

- letter of representation
- certificate of Incorporation (or equivalent document)
- letter of financial auditor
- annual reports of last 3 years with financial statements
- articles of association and by-laws (or equivalent)
- tax certificate or registration (or equivalent)
- insurance certificate covering professional liability for an amount of at least 1 (one) million euros
- board of directors and representatives that are authorised to sign on behalf of the applicant company towards third parties
- list of shareholders/owners with details of the ultimate shareholders/owners

Based on the received documentation, SWIFT assesses compliance with the legal and financial eligibility criteria. The financial compliance check includes the analysis of the financials and (for applicants that are SWIFT customers or have a pre-existing relationship with SWIFT) the payment history of SWIFT invoices.

In conducting the assessment, SWIFT may solicit the views of the relevant National Member or User Group or those entities within the same group of companies as the applicant that are already admitted under the Enabler Programme.

Good payment behaviour is defined as a settlement of all undisputed invoices within the standard credit settlement terms of 30 days net date of invoice. Any Partner that with respect to any SWIFT invoices accrues more than 60 days overdue more than three times in any calendar year or fails to pay fees within 90 days of the due date is considered to be in non-compliance with the legal and financial eligibility criteria.

If a Partner is a SWIFT shareholder or is SWIFT shareholder-owned, then the legal and financial assessments are executed as part of a separate process (that is, the continued due diligence checks on such SWIFT shareholder(s)).

SWIFT reserves the right to supplement the above requests for information or documentation as it deems necessary or advisable.

The outcome of the assessment can be either of the following:

- Compliant: the application is compliant with the above-mentioned eligibility criteria.
- Non-compliant: the application is rejected. A notification is sent to the applicant. An application can also be rejected based on a time-out implying the failure of the applicant to provide complete documentation and information in a timely manner.

FOR PARTNERS ENABLING SERVICES THROUGH APIs:

Part 1 – Technical Validation

SWIFT API knowledge exam

All Partners must demonstrate a fundamental understanding and awareness of SWIFT's API offering, including but not limited to:

- API specifications and authentication methods,
- API versioning and life cycle
- SWIFT API components (such as SDK and/or Microgateway)
- SWIFT Developer Portal API Sandbox

Each Partner is expected to have relevant members of their staff (at minimum one) complete an examination process to validate that their developers, solution architects and other relevant personnel are familiar with the key principles required to properly deliver a quality offering to SWIFT customers/End Users.

Further details on the steps to complete this process are available on swift.com.

SWIFT API sandbox testing

All Partners are expected to use the SWIFT Developer Portal API Sandbox to complete the prerequisite test scenario as defined for the particular SWIFT API service they intend to distribute/integrate as contemplated by the Enabler Programme. These requirements will include, but are not limited to:

- Successful implementation and configuration of the SWIFT SDK or Microgateway
- Creation of the appropriate consumer secrets/keys in SWIFT Developer Portal
- Initiate successful API requests with response
- Initiate API request to trigger an error response, and interpret alert to take corrective action accordingly

The full list of requirements for a given SWIFT Service are identified on swift.com

SWIFT end-to-end service scenario testing

For some SWIFT Services, the Partner may be mandated to successfully complete a number of end-to-end user scenarios with the SWIFT Test Sparring Partner in our Test and Training environment.

This is specifically required when the SWIFT Service is directly interacting with the SWIFT messaging services, and thus requires additional testing in addition to what is available in the API sandbox. Where

relevant, SWIFT will provide reasonable assistance to the Partner to help facilitate the completion of this exercise.

Further details on the steps to complete this process are available on swift.com.

Part 2 – Functional Validation

Solution architecture topology

SWIFT requires each Partner to share a high-level schematic of how they intend to integrate the SWIFT SDK and/or Microgateway component(s) into their proposed solution architecture.

This solution architecture proposal will be validated by SWIFT to help assure the appropriate level of functioning and scalability of the offering which will incorporate SWIFT Services.

Operational demonstration of solution's capabilities

The Partner will organise a demo of the operation of their solution, specifically in relation to the integrated SWIFT Service and the value-added functionality it provides to the SWIFT customer.

Additional detailed information regarding the accreditation process can be found on the relevant pages of the SWIFT Partner Portal (on swift.com).

Note: the accreditation process defined herein is only qualifying the ability of a business application or solution or middleware to successfully interact with the SWIFT Service through APIs. It is not qualifying any formal adherence to SWIFT Service terms or requirements. SWIFT makes available additional accreditation labels (such as the SWIFTgpi and SWIFTgpi for Corporates) which do validate those requirements. Partners can choose to undertake those accreditations.

In cases of any material non-compliance with any aspect of the Partner Accreditation Process, SWIFT reserves the right to (1) notify End Users accordingly; and/or (2) de-list the Partner from any listings or collateral or similar material relating to the Enabler Programme. During such time as a Partner may be so de-listed, the Partner may not, without SWIFT's prior written consent, sign up or subscribe to the Enabler Programme any new or additional End Users. Any such right of SWIFT is part of an "escalation process" as referenced in the Enabler Terms and Conditions.

FOR PARTNERS ENABLING CONNECTIVITY THROUGH BUSINESS CONNECT SOLUTION:

BUSINESS ELIGIBILITY CRITERIA

During the qualification process, the applicant shall provide the following details:

- Name of the Business Application Model
- Target market segment(s): Corporates, Securities, Trade, and so on

- Number of customers using the Business Application Model
- Number of expected new customers to use SWIFT through the Business Connect Solution per year
- Region(s) where you wish to offer integrated Business Connect Solution: Americas, EMEA and/or Asia Pacific
- Company revenue in the previous year
- Existing customer references for Enabler Programme
- Existing SWIFT capabilities of the Business Application Model
- Supported SWIFT message sets
- Additional message sets (if any)
- Brief explanation of Business Application Model functionality
- The business segments which are of interest
- Information relevant to any other SWIFT service or product that SWIFT may consider allowing Partner to make available to End Users as part of the Enabler Programme

When the above-mentioned information has been validated by SWIFT, a demo of the Business Application Model will be required and an approval notification from the targeted business market segment.

Following a positive first assessment, SWIFT asks the potential Partner to submit the required additional documentation to perform the legal and financial compliance checks. If the original documentation is not in English, then the applicant is requested to provide, in addition to the original documentation, an English translation of the document. SWIFT reserves the right to supplement the above requests for information or documentation as it deems necessary or advisable.

Following a negative first assessment, SWIFT sends a rejection notice to the applicant.

BUSINESS APPLICATION MODEL QUALIFICATION

The Business Application Model of the Partner must meet a set of predefined criteria for a selected business segment. The applicant must undergo the qualification of its Solution annually and fulfil the criteria as set out below in the “COMPATIBILITY OF BUSINESS APPLICATION MODEL” section.

COMPATIBILITY OF BUSINESS APPLICATION MODEL

Qualification of the Business Application Model as being SWIFT Compatible falls under and must always comply with the technical and functional validation parameters prescribed by SWIFT.

Focus

The Business Application Model that is the subject of the qualification must operate to the satisfaction of SWIFT and its users. The software must meet a set of predefined criteria for a selected business segment, which validates the software capability to provide Straight-Through Processing (STP) and value-added services for SWIFT messaging.

SWIFT does not qualify dedicated models/solutions that are developed for particular End Users or models/solutions that need a high degree of customisation prior to implementation.

Qualification of a Business Application Model is granted for a period of one year and must be renewed annually. The qualification criteria for a business segment may change from year to year to reflect market

evolution and End User needs. In case of criteria changes, SWIFT may require re-validation. In selective cases, only technical validation is required for renewal. SWIFT maintains discretion to mandate re-qualification of the solution following a major release change to the software.

The technical and functional validation tests SWIFT-specific features of the product. It is not meant to replace any product acceptance testing the Partner must pursue within its organisation before submitting the application to this Programme.

Process

The Partner reviews the relevant criteria documents from SWIFT for a preferred business segment and informs SWIFT of the message types or sets which it wishes to be qualified for. SWIFT then analyses the request and determines whether the Business Application Model satisfies the set of criteria, as applicable.

If the criteria are met, the Partner and SWIFT prepare for a technical validation. The Partner runs the required product tests according to the business segment specifications with the SWIFT qualification team. After a successful technical validation, the Partner performs the functional validation. By means of a webinar, the Partner presents a detailed demonstration of the Business Application Model to SWIFT business experts who then assess compliance with SWIFT's functional validation criteria. The content of the presentation is agreed upon beforehand.

After successful functional validation, the Business Application Model is approved to go live. Once the first End User is successfully implemented, the Business Application Model is considered qualified.

NOTWITHSTANDING THE QUALIFICATION/VALIDATION OF A BUSINESS APPLICATION MODEL AS CONTEMPLATED IN THIS ANNEX, PARTNER MUST ASSURE AT ALL TIMES THAT IT HAS VALIDATED THE TECHNICAL COMPATIBILITY OF ITS BUSINESS APPLICATION MODEL(S) WITH ALL RELEVANT ASPECTS OF THE MESSAGE TYPES THAT ARE INCLUDED IN THE MESSAGING SETS IT WILL ENABLE OVER ITS BUSINESS APPLICATION MODEL(S) AND THAT IT IS MONITORING ALL NEW SWIFT STANDARDS RELEASES AND OTHER SWIFT SERVICE OR PRODUCT UPDATES/RELEASES/NEW VERSIONS AND MAKING APPROPRIATE ADJUSTMENTS TO ITS BUSINESS APPLICATION MODEL(S) SO AS TO ASSURE THAT ALL MESSAGE TYPES SENT OR RECEIVED BY END USERS OVER ITS BUSINESS APPLICATION MODEL(S) WILL FLOW SMOOTHLY AND WITHOUT INTERRUPTION AND WITHOUT SUCH MESSAGE TYPES BEING "NAKED" OR IMPEDED OR ADVERSELY AFFECTED IN ANY WAY DUE TO THE BUSINESS APPLICATION MODEL(S) NOT BEING COMPATIBLE WITH SUCH MESSAGE TYPES.

Compliance with the foregoing, as in effect from time to time, is a requirement of the Agreement between SWIFT and each Partner.

ANNEX 3

END USER POLICY

SWIFT may amend this Policy from time to time by publishing the new version on swift.com or otherwise making such new version available to End Users.

INTRODUCTION

SWIFT is active in the field of secure messaging services and offers various services and products supporting or complementary or ancillary to such messaging services.

The technology solution provider you have engaged supplies a technology solution to its customers (hereafter referred to as 'End Users') and has opted to integrate or embed certain SWIFT services or products with or in that solution offering.

SWIFT has developed a Programme (hereafter referred to as the 'Enabler Programme') whereby such technology solution providers can enable End Users that are also SWIFT customers to access certain SWIFT services or products through SWIFT APIs and, in addition, certain technology solution providers may have qualified to provide the Business Connect Solution to End Users that are SWIFT users so as to enable such End Users to connect to the SWIFT messaging network through SWIFT's Alliance Cloud service. The Enabler Programme is designed to provide easy and convenient access to such SWIFT services or products. End Users must be SWIFT customers (and must be qualified as SWIFT users in the case of the Business Connect Solution) in order to access SWIFT services or products as contemplated by the Enabler Programme and subscribe to such services or products with SWIFT. The Enabler Terms and Conditions can be found on swift.com.

Unless the context indicates otherwise, capitalised terms used in this document and not otherwise defined have the meanings assigned to them in the Enabler Terms and Conditions.

PURPOSE OF THIS DOCUMENT

This document sets out SWIFT's policy with respect to a SWIFT customer wishing to use certain SWIFT services or products through a technology solution provider (hereafter an "Enabler Partner"; referred to in the Enabler Terms and Conditions as a "Partner") that participates in the Enabler Programme. To that end, SWIFT customers will rely on the Enabler Partner when consuming SWIFT services or products in conjunction with the Enabler Partner's Partner Service.

This *End User Policy* forms an integral part of the contractual terms between SWIFT and its users and customers. It must be read along with any other specific terms and conditions relating to the provision of the SWIFT Services that you access through the Service Enablement of the Enabler Partner , as specified in the relevant SWIFT contractual documentation (typically a service description for the SWIFT Service, together with the SWIFT General Terms and Conditions, or a document setting out the terms and conditions for the SWIFT Service; the SWIFT API Gateway Service Description, SWIFT Software Development Kit Service Description and/or the SWIFT Microgateway Service Description will be relevant to the consumption of SWIFT Services through SWIFT APIs; for the Business Connect Solution, the SWIFT Alliance Cloud Service Description will be relevant).

AUDIENCE

This document is intended for the following audience:

- SWIFT customers wishing to understand the policy that governs the use of an Enabler Partner to access a SWIFT Service.

- Enabler Partners participating in the Enabler Programme

This Policy will be available on swift.com and may be amended from time to time by SWIFT. In any event, SWIFT may amend this Policy from time to time by publishing the new version on swift.com or otherwise making such new version available to End Users.

SWIFT-DEFINED TERMS

In the context of SWIFT documentation, certain terms have a specific meaning. These terms are called SWIFT-defined terms (for example, *customer*, *user*, or SWIFT services and products). The definitions of SWIFT-defined terms appear in the SWIFT Glossary.

Related documentation

- Partner Programme Terms and Conditions
- Enabler Programme Terms and Conditions
- SWIFT General Terms and Conditions
- SWIFT Corporate Rules
- SWIFT By-laws
- SWIFT Personal Data Protection Policy
- SWIFT Software Development Kit Service Description (for End Users accessing SWIFT Services through SWIFT APIs)
- SWIFT Microgateway Service Description (for End Users accessing SWIFT Services through SWIFT APIs)
- SWIFT API Gateway Service Description (for End Users accessing SWIFT Services through SWIFT APIs)
- Alliance Cloud Service Description (for End Users obtaining connectivity to the SWIFT network through the Business Connect Solution)
- the applicable SWIFT contractual documentation for the SWIFT service being accessed
- SWIFT Customer Security Controls Framework
- SWIFT Customer Security Controls Policy
- Customer Security Programme Terms and Conditions
- Know your Customer – Security Attestation (KYC-SA)

THE ENABLER PROGRAMME

1.1 Overview

As mentioned above, the Enabler Programme is intended to enable Enabler Partners to pair SWIFT Services with Partner Services in order to enable End Users that are also SWIFT customers (SWIFT users in the case of the Business Connect Solution) to access these SWIFT Services through the Enabler Partner. As set out in the Enabler Terms and Conditions, Enabler Partners may do this by using a Business Application Model or an API Concentrator Model. The API Concentrator Model may involve Distribution Elements other than the Enabler Partner. End Users should understand from their Enabler Partner which model is being used and which, if any, Distribution Elements or distribution channels for the SWIFT Services may be relevant.

The Enabler Programme includes eligibility criteria as well as a SWIFT accreditation of the Partner Service into which the SWIFT Service will be embedded or integrated and the need for the Enabler Partner to comply with certain qualification criteria, including, in some cases, SWIFT operational and security requirements. Details concerning the eligibility criteria and the accreditation process, as well as SWIFT operational and security requirements, are referenced in the Enabler Terms and Conditions that can be found on swift.com or upon request to SWIFT.

1.2 General Principles

It is incumbent upon the End User to assure itself that it understands the model and any distribution channels or Distribution Elements being used by the Enabler Partner and that the Enabler Partner has instituted appropriate operational and security and service level terms and procedures to assure the smooth and proper functioning and provision of SWIFT Services being facilitated by the Enabler Partner through its Service Enablement.

The Enabler Partner is not entitled to use for its own purposes or benefit SWIFT Services that are the subject of its Service Enablement. Likewise, security features, including certificates of End User's identity, allocated to End Users, are not intended to be used by an Enabler Partner for its own benefit except when performing testing on an isolated test bed environment and with the End User's consent.

End Users understand that depending upon various circumstances, including, but not limited to, the SWIFT Service(s) being distributed to them through the Service Enablement of an Enabler Partner, as well as the functional/operational role of the Enabler Partner in distributing such SWIFT Service(s), an Enabler Partner may have access to confidential information and/or data of the End User or its customers or staff in connection with carrying out its role as Enabler Partner. It is the responsibility of End User to put in place appropriate controls and safeguards to address this issue.

The End User must be aware that granting any staff of the Enabler Partner an official SWIFT capacity on behalf of End User (such as "API Administrator" or "security officer") will confer a wide range of authority upon such Enabler Partner staff member to act in the name of End User. The decision to do so, and the imposition of appropriate controls with regard to the Enabler Partner, is the sole responsibility of the End User.

Acts and Omissions of Enabler Partner or Distribution Element, and so on.

End Users acknowledge and understand that the introduction of an intermediary (such as an Enabler Partner or Distribution Element) introduces potential risk for interruption or disruption of the SWIFT Service(s) they wish to consume through the Enabler Programme. End Users understand and agree that SWIFT is not responsible or liable for the acts, omissions, performance or errors of the Enabler Partner or any Distribution Element or any Partner Service or application or solution or middleware used by an Enabler Partner or End User with respect to the distribution of any SWIFT Service that is consumed by an End User through an Enabler Partner as contemplated by the Enabler Programme. SWIFT is not responsible or liable for any malfunction, corruption or unavailability of a SWIFT Service due to any such act, omission, performance or error.

1.3 End User's Roles and Responsibilities

Responsibility when consuming SWIFT Services through an Enabler Partner

End Users that decide to use SWIFT Services through the Service Enablement of an Enabler Partner do so based upon their own assessment of that Enabler Partner and the distribution model used by such partner (Business Application Model or API Concentrator Model) and under their own responsibility. SWIFT disclaims any liability or responsibility whatsoever for the acts, faults, or omissions of the Enabler Partner or any aspect of such partner's Partner Service, Service Enablement or any aspect of a Distribution Element.

It is important to note that while SWIFT engages in a limited degree of compatibility and integration testing of the Enabler Partner's Partner Service with relevant SWIFT Services and SWIFT APIs, it is ultimately the sole responsibility of the Enabler Partner to validate, test for and assure such compatibility initially and on an ongoing basis.

SWIFT disclaims any liability for any failure by an Enabler Partner to assure that (1) SWIFT Services and SWIFT APIs are interoperable and properly synced and compatible with the relevant Partner Service and (2) the model of distribution selected by the Enabler Partner (Business Application Model and/or API

Concentrator Model) functions smoothly, properly and without corruption or impairment of SWIFT Services or SWIFT APIs. An End User must assure itself that any technical, functional, security or operational responsibilities being assumed by an Enabler Partner (or any third party or relevant Distribution Element) with regard to any SWIFT Services are being carried out in a manner that is prudent and consistent with all relevant SWIFT contractual documentation and being carried out in a manner that is secure and functionally and operationally sound.

SWIFT encourages and expects any End User considering using a Partner Service and an Enabler Partner as a distribution channel for SWIFT Services to undertake all due diligence that the End User believes is necessary or prudent.

An End User that leaves, or changes (or intends to leave or change) its Partner Service must promptly inform SWIFT with, to the extent possible, at least three months advance notice of its intention to do so. An End User no longer using (or allowed to use) a Partner Service must make any necessary arrangements with SWIFT to migrate any SWIFT Service paired with such Partner Service to another Enabler Partner or to a direct relationship with SWIFT.

Responsibility to adhere to Customer Security Programme

SWIFT customers must adhere to the Customer Security Programme. For the components that fall under the scope of the Enabler Partner, the relevant Security and Operational Requirements apply.

Removal of an Enabler Partner

Should SWIFT remove an Enabler Partner from its Enabler Programme, SWIFT will use commercially reasonable efforts to notify the impacted SWIFT customers at least three months in advance (or, in circumstances not permitting three months' notice, as much advance notice as possible) of the removal of their Enabler Partner from the Enabler Programme. Such a removal does not affect the End User's right to continue to use SWIFT Services. However, it will be necessary for the End User to migrate to an alternative distribution channel or method in order to continue to consume such SWIFT Services.

Removal of an End User by an Enabler Partner

End Users understand and agree that their Enabler Partner may terminate their appointment to provide SWIFT Services in conjunction with the Partner Service, by, to the extent possible, notifying the terminated End User and SWIFT at least three months in advance. End Users understand that they will have contracts with their Enabler Partner that are outside the responsibility and control of SWIFT and the terms of which are not known to SWIFT. End Users no longer allowed to use a Partner Service must make any necessary arrangements with SWIFT to migrate any SWIFT Service paired with such Partner Service to another Enabler Partner or to a direct relationship with SWIFT.

Other End User responsibilities

The Enabler Partner will in principle represent its End Users in dealing with SWIFT. However, SWIFT remains a direct contact towards its End Users for any matter related to SWIFT usership/membership and the SWIFT Services, including matters related to SWIFT's Customer Security Programme.

An End User must ensure that the scope of rights that it grants to its Enabler Partner in respect of SWIFT Services is aligned with applicable SWIFT contractual documentation. Also an End User must ensure that its Enabler Partner is bound by no less stringent obligations than those incumbent upon the End User under its contractual documentation with SWIFT.

An End User remains responsible to SWIFT for due performance and observance by its Enabler Partner of those of its obligations owed to SWIFT that the End User may delegate or sub-contract to the Enabler Partner. In particular, a failure by the Enabler Partner selected by its End User to comply with these obligations may result in the suspension or the termination of the End User's access to and use of the SWIFT Services through such Enabler Partner.

In particular, the End Users have the following responsibilities:

- Control how the Enabler Partner manages access to, and the use of, the SWIFT Services and, in particular, ensure that all security features allocated to the End User to secure its access and use of the SWIFT Services are securely operated and kept safe to prevent any unauthorised access to or use of the SWIFT Services.

- Ensure that the Enabler Partner maintains and documents an acceptable level of security procedures and standards with respect to data privacy, data separation, confidentiality, integrity, and systems availability.

- Ensure that the Enabler Partner is bound by no less stringent obligations of confidentiality and use of information and data than those applicable to End User as a SWIFT customer in respect of information and data related to SWIFT Services; assure that any contractual requirements of the relevant SWIFT Service relating specifically to partners or third parties are observed by the Enabler Partner to the extent applicable.

- Ensure all necessary technical, operational and functional processes relevant to distribution or execution or Service Enablement of SWIFT Services are carried out by the Enabler Partner accordingly.

- Should End User participate in an API Concentrator Model, it will provide SWIFT and/or Enabler Partner with any relevant information about Distribution Elements that are under End User's control or responsibility, to the extent necessary to assure smooth distribution and functioning of SWIFT Services subscribed by End User.

Customer Security Controls Framework and Customer Security Controls Policy

While customers are responsible for protecting their own environments and access to SWIFT, SWIFT has published the Customer Security Controls Framework (CSCF) and the SWIFT Customer Security Controls Policy (CSCP) to support SWIFT customers in the fight against cyber fraud. The CSCF establishes a common set of mandatory and optional security controls designed to help customers to secure their local environments and to foster a more secure financial ecosystem. The CSCP describes the obligation for SWIFT customers to self-attest against the SWIFT security controls set out in the CSCF. End Users, like all SWIFT customers, are responsible for meeting their obligations under the CSCP and CSCF.

Confidential information

End Users agree that SWIFT may share their confidential information with their Enabler Partner and that the Enabler Partner can also share such information with SWIFT, for the execution of their respective contractual obligations and for legitimate purposes, such as provisioning, support, security, operational, or reporting purposes or in order to market any SWIFT products or services that could meet the needs of the End Users.

1.4 Enabler Partner requirements

All Enabler Partners willing to participate in the SWIFT Enabler Programme must fulfil the criteria and requirements set out in the Enabler Terms and Conditions, including, but not limited to, registration to, and compliance with, the SWIFT Partner Programme and the Partner Programme Terms and Conditions and must have their Partner Service qualified, as contemplated by the Partner accreditation process set out in the Enabler Terms and Conditions. Failure by the Enabler Partner to comply with such criteria and requirements may result in its being terminated from the Enabler Programme and result in an End User

having to make alternative arrangements for consumption of any SWIFT Services being consumed as contemplated by the Enabler Programme.

Service level agreement implementation

The Enabler Partner must provide End Users with a service level agreement consistent with the Enabler Programme and the particular SWIFT Services being accessed by the End User through the Enabler Partner.

1.5 Centralised Billing

SWIFT may (but is not obligated to) allow Centralised Billing for some SWIFT Services and/or some Enabler Partners. Allowing Centralised Billing for one SWIFT Service made available through a particular Enabler Partner does not imply that any other SWIFT Services offered through such Enabler Partner will be permitted to use Centralised Billing. To the extent that SWIFT agrees with an Enabler Partner to allow Centralised Billing, for those End Users of an Enabler Partner that has agreed with SWIFT that Enabler Partner will provide Centralised Billing whereby Enabler Partner will be invoiced, and make payment, for certain SWIFT services and products used by its End Users, the following paragraph applies:

For a predefined set of SWIFT products and services that will be offered by the Enabler Partner to its End Users and ordered by the Enabler Partner on behalf of its End Users, SWIFT will invoice the Enabler Partner, and the Enabler Partner will pay all fees and charges due for the use of these SWIFT services and products by the End Users. In such case, the Enabler Partner will act as an intermediary in the sense of article 28 of the EU VAT directive. If the Enabler Partner does not pay all such fees and charges in a timely manner, then SWIFT is entitled to suspend or terminate the provision of SWIFT services and products to the End Users concerned. In the event that Centralised Billing is terminated for any reason, SWIFT will invoice End Users directly for the fees and charges previously invoiced to the Enabler Partner in connection with such Centralised Billing.

1.6 For End Users participating in the Business Connect Solution

In addition to the other terms of this End User Policy, End Users that obtain connectivity to SWIFT messaging services through an Enabler Partner through the Business Connect Solution agree to the following terms as they relate to the Business Connect Solution. As mentioned, the Business Connect Solution is provided by means of SWIFT's Alliance Cloud service and End Users will be subscribers to the Alliance Cloud Service per the terms and conditions of the Alliance Cloud Service Description and the SWIFT General Terms and Conditions.

For the Business Connect Solution, it is within the Enabler Partner's discretion to determine exactly what types and sets of messages the Enabler Partner will enable an End User to send or receive through its Partner Service. Under certain circumstances SWIFT may limit or restrict the range of message types or sets permitted to be sent through the Partner Service. It is important to note that while SWIFT engages in a limited degree of compatibility testing of the message sets that the Enabler Partner will be permitted to allow through its Partner Service, it is ultimately the sole responsibility of the Enabler Partner to validate, test for, and assure such compatibility initially and on an ongoing basis.

End Users that decide to connect to the SWIFT messaging network through an Enabler Partner do so under their own responsibility. SWIFT disclaims any liability for any failure by Enabler Partner to assure that message types and sets allowed to be sent or received through its Partner Service may be transmitted smoothly, properly and without corruption through any Partner Service. With respect to SWIFT's Alliance

Cloud service, an End User must assure itself that any functional or operational responsibilities being assumed by Enabler Partner with respect to any such service are being carried out in a manner that is prudent, secure and consistent with all relevant SWIFT contractual documentation.

If an End User decides to use two or more Enabler Partners, it will have to order separate BICs to be associated with the respective Enabler Partners.

End Users have the following responsibilities:

- Control how the Enabler Partner manages access to, and the use of, the SWIFT messaging services and, in particular, ensure that all security features allocated to the End User to secure its access and use of the SWIFT messaging services are securely operated and kept safe to prevent any unauthorised access to or use of the SWIFT messaging services.

- Ensure that the Enabler Partner maintains and documents an acceptable level of security standards for message confidentiality, integrity, and systems availability.

- Ensure that the Enabler Partner is bound by no less stringent obligations of confidence than those applicable to End User as a SWIFT user in respect of information related to SWIFT services and products or, more generally, SWIFT operation.

- Select and use an Enabler Partner which has and maintains an accredited/qualified Partner Service at all times.

- Ensure all traffic that is intended to go to the SWIFT messaging services is processed by the Enabler Partner accordingly.

Responsibility to adhere to Customer Security Programme

SWIFT users must adhere to the SWIFT Customer Security Programme. A user connected to the SWIFT network through an Enabler Partner must attest compliance against all mandatory security controls as documented in the Customer Security Control Framework (CSCF) in effect at the time of publication of the attestation. End Users must attest for all in-scope components in their local environment according to their architecture type as described in the CSCF. For the components that fall under the scope of the Enabler Partner, the Provider Security Controls Framework applies. The compliance status of the Enabler Partner is visible in the SWIFT Business Connect Directory on swift.com and in the Know Your Customer Self-Attestation (KYC-SA) application.

Responsibility to secure the connection to a Enabler Partner

It is a joint responsibility of the End User and the Enabler Partner to secure the connection to an Enabler Partner. When connecting to an Enabler Partner, some PSCF controls may be more restrictive than the CSCF controls applicable to End User.

Removal of an Enabler Partner

In the exceptional case that SWIFT would remove an Enabler Partner from its Enabler Programme, SWIFT will use all commercially reasonable efforts to notify the impacted End Users at least three months in advance (or, in circumstances not permitting three months' notice, as much advance notice as possible) of the removal of its Enabler Partner from the Enabler Programme. Such a removal does not affect the End User's right to continue to use the Alliance Cloud service to send messages directly with SWIFT, that is, without going through the Partner Service. It may be necessary for the End User to migrate certain SWIFT services and products to a direct subscription with SWIFT. In due time, the invoice for the SWIFT related fees will then be sent to the End User directly instead of the Enabler Partner.

An End User's responsibility for all messages sent and received, and so on.

To avoid any doubt, End Users as identified on SWIFT through their own BIC remain fully responsible for all messages sent or received by them or operations performed under their BIC through an Enabler Partner. In particular, SWIFT users recognise that the delivery of a message or file to the Alliance Cloud portal (or the equivalent in the case of any on-premises connectivity infrastructure) operated by an Enabler Partner is considered to be a delivery of that message to them.

Use of an Enabler Partner does not affect the responsibility of the End User for all messages emanating from the End User and identified by the BIC8 of the End User.

End Users also acknowledge that the types or sets of SWIFT messages that can be sent through an Enabler Partner are limited and depend on the particular Partner Service they are using. The list of authorised SWIFT message types or sets for a Partner Service is made available to the End Users by SWIFT or the Enabler Partner upon request.

End Users have also the option to send messages through Alliance Cloud directly to SWIFT when not using the applicable Partner Service.

End Users acknowledge that should they send or receive any SWIFT messages, whether of a type authorised in connection with a particular Partner Service or otherwise, the Enabler Partner will have access to such messages, except to the extent SWIFT has agreed with End User to implement (and has implemented) customised set-ups and/or configurations with respect to the messages in question.

We confirm our agreement with the End User Policy:

Name of End User: _____

By_____

Name:

Title:

Date:

ANNEX 4

SWIFT Services and Related Terms

SWIFT reserves the right to amend/update from time to time these SWIFT Services and Related Terms upon prior notice to Partner (including notice by either e-mail and/or by posting a new version on www.swift.com).

A Partner that participates in the SWIFT Enabler Programme will be permitted to embed/integrate with its Partner Service those SWIFT Services that have been indicated per the Partner Schedule (as may be updated from time to time) and for which Partner has been expressly permitted per the Enabler Terms and Conditions.

Except as noted below for the Business Connect Solution, a Partner will access SWIFT Services through SWIFT APIs, per the terms of the relevant SWIFT Service Description (or other relevant contractual documentation), and per the terms of the **SWIFT API Gateway Service Description**, **SWIFT Software Development Kit (SDK) Service Description** and/or the **SWIFT Microgateway Service Description**. In addition, SWIFT will facilitate connectivity to its messaging services through the Alliance Cloud solution as per the Alliance Cloud Service Description (such facilitation of connectivity is referred to as the Business Connect Solution). When doing so, the Partner must act in compliance with the contractual terms of the relevant SWIFT Service, with particular attention to carrying out any functional or operational obligations; observing any terms having to do with confidentiality and security and use of data or information; and complying with any applicable service level or similar requirement.

The list of SWIFT Services and corresponding contractual documentation is as follows (referenced documents may be found on swift.com):

(as of July 1st, 2023)

SWIFTRef PRODUCTS AND SERVICES

- SWIFTRef Product Terms and Conditions
- SWIFTRef Licence Terms and Conditions

gpi AND gpi TRACKER

- SWIFT gpi Service Description; SWIFT General Terms and Conditions

PAYMENT PRE-VALIDATION

- Payment Pre-validation Service Description; SWIFT General Terms and Conditions

KYC REGISTRY

- KYC Registry Service Description; SWIFT General Terms and Conditions

TRANSACTION SCREENING

- Transaction Screening Service Description; SWIFT General Terms and Conditions

WATCH BANKING ANALYTICS

- Watch Banking Analytics Service Description; SWIFT General Terms and Conditions

COMPLIANCE ANALYTICS

- Compliance Analytics Service Description; SWIFT General Terms and Conditions

ALLIANCE CLOUD (as used in Business Connect Solution)

- Alliance Cloud Service Description; SWIFT General Terms and Conditions

Contractual documentation for SWIFT Services is available through the Knowledge Centre of swift.com. In case of questions or doubt, please contact your SWIFT Account Manager

ANNEX 5

Fees/Financial Conditions

Pricing and fees, as well as any other financial conditions, are as published in the SWIFT price list or furnished by quotation or otherwise notified in writing by SWIFT, all as may be amended from time to time by SWIFT, upon prior notice to Partner (including notice by e-mail and/or by posting on www.swift.com)

ANNEX 6

MUTUAL NDA

Each party wishes to protect its information which will come to the other party's knowledge in the context of the discussions, communications and other arrangements between the parties in connection with the performance and execution of the Agreement (hereafter referred to as the "**Purpose**").

1. **Agreement**

   In consideration of a party (hereafter referred to as the "**Disclosing Party**") agreeing to disclose or procure the disclosure of certain information to the other party (hereafter referred to as "the **Receiving Party**") from time to time in connection with the Purpose, the parties agree that the following terms and conditions shall apply to all disclosures of Confidential Information in relation to or in any way concerning the Purpose.

2. **Confidential Information**

   Any information, data and/or materials of whatever kind or nature (or any portion thereof) that may become known to the Receiving Party or is otherwise transmitted to the Receiving Party in connection with the Purpose, by whatever means and in whatever form (including (but not limited to) information and/or data communicated orally), related to the Disclosing Party or any of its Affiliates (as defined herein) or their respective business operations or customers (hereafter referred to as "the **Confidential Information**"), shall be considered as confidential and proprietary to the Disclosing Party and, without prejudice to the other terms of this NDA shall be treated as such by the Receiving Party.

   The Confidential Information includes (without limitation) inventions, products, services, strategy, personnel, methods of doing business, research and development activities, know-how, customers, shareholders, trade secrets, commercial secrets, computer programs or finances.

   The Confidential Information may also include information which has been submitted to the Disclosing Party by third parties, and which the Disclosing Party has been authorised to disclose, subject to security measures or confidentiality provisions, or other agreements. In such case, the Receiving Party accepts that the terms of this NDA shall be deemed to be also for the benefit of the Disclosing Party and any such third parties.

   However, the Confidential Information does not include information that the Receiving Party can prove by written records:

   (1) was in the public domain at the time it became known or was transmitted to the Receiving Party;

   (2) becomes part of the public domain thereafter through no breach of this NDA;

   (3) was already in the Receiving Party's possession free of any obligation of confidentiality; or

   (4) was developed by the Receiving Party independently without use of any Confidential Information.

3. **Protection of Confidential Information**

   The Receiving Party shall ensure the protection, confidentiality and security of the Confidential Information using the same standard it employs to safeguard its own information of like kind, but in no event less than a reasonable standard of care.

4. **Use of Confidential Information**

   The Receiving Party shall not use or copy the Confidential Information for any purpose other than the Purpose and, subject to clause 5, shall neither directly nor indirectly disclose or permit such Confidential Information to be made available to any third party without prior written authorisation from the Disclosing Party.

5. **Disclosure of Confidential Information**

The Receiving Party undertakes that it will only disclose any Confidential Information to those of its or its Affiliates' employees, directors, agents, subcontractors, professional advisers or, subject to the approval of the Disclosing Party referred to in clause 4, any other third party (hereinafter "the **Authorised Parties**") who need to know the Confidential Information for the Purpose, always subject to the following:

(1) Prior to disclosing any Confidential Information to Authorised Parties the Receiving Party will:

(a) inform the Authorised Parties of the restrictions as to use and disclosure of the Confidential Information contained in this NDA; and

(b) ensure that the Authorised Parties are bound by a confidentiality undertaking or obligations of confidence which protect the Confidential Information to at least the extent that it is protected under this NDA; and

(2) The Receiving Party will procure that the Authorised Parties observe the terms of the undertaking or, as the case may be, obligations of confidence referred to above.

However, the Receiving Party shall not be deemed to be in breach of this NDA if it discloses or otherwise makes the Confidential Information available in response to a bona fide subpoena or other lawful process by a court or regulatory, supervisory or governmental authority of competent jurisdiction, provided however that the Receiving Party shall, if and to the extent permitted by applicable law, (1) notify the Disclosing Party without delay of any such process; (2) use reasonable efforts to maintain the protection, confidentiality and security of the Confidential Information; and (3) co-operate with and assist the Disclosing Party so as to allow the Disclosing Party to seek any legal remedies it may deem appropriate to protect the Confidential Information.

It is understood that Confidential Information may be disclosed to an End User receiving SWIFT and Partner's services/products as contemplated by the Agreement, but only to the extent reasonably necessary to properly provide services/products to such End User.

"Affiliate" means any other entity Controlling, Controlled or under common Control with the Receiving Party. "Control" and its derivatives shall mean the holding, directly or indirectly, more than 50% ownership interest.

6. **No Representations or Warranties**

All Confidential Information is made available on an "as is" basis and all representations and warranties, express or implied, are hereby disclaimed. Without limitation to the foregoing, the Disclosing Party disclaims all representations and warranties with respect to the following matters: (1) that the Confidential Information is accurate, complete and reliable for any purpose whatsoever and (2) any warranties of merchantability or fitness for a particular purpose.

7. **No License or Conveyance**

Nothing in this NDA shall convey to the Receiving Party any right, title, interest or license in or to any information (including any Confidential Information) that may become known to the Receiving Party or is otherwise transmitted to the Receiving Party in connection with the Purpose, or in or to any trademark, trade name, or any other intellectual property rights of the Disclosing Party.

8. **Return or Destruction of Confidential Information**

Upon the written request of the Disclosing Party, the Receiving Party shall, at the Disclosing Party's option, promptly return or destroy all documents and other materials in whatever form containing, relating to or derived from the Confidential Information. The Receiving Party shall however be entitled to retain copies or records of the Confidential Information to the extent required by any applicable law or regulation.

9. **Duration**

The obligations of the parties contained in this NDA shall survive the parties' termination of their business relationship in connection with the Purpose and shall remain in full force and effect thereafter.

ANNEX 7

Service Enablement of Business Connect Solution

The following terms apply to a Partner using SWIFT's Alliance Cloud connectivity solution ("Alliance Cloud") to provide the Business Connect Solution to End Users. While the main body of the SWIFT Enabler Programme Terms and Conditions will apply to such a Partner, the Partner will also be subject to the terms of this Annex with respect to any activities or matters related to its Service Enablement of the Business Connect Solution.

INTRODUCTION

In order to use the Business Connect Solution, End Users must apply to become, and must be accepted by SWIFT as, and remain, SWIFT users, and must subscribe to SWIFT's Alliance Cloud connectivity solution.

SWIFT's Business Connect Solution enables a Partner offering its Business Application Model to customers and wishing to procure the use of Alliance Cloud for such customers that become End Users to pair Alliance Cloud with Partner's Business Application Model. The Business Connect Solution focusses on a Business Application Model's technical compatibility with certain sets of SWIFT messages and SWIFT message services (for example, such message set may include all MTs 100 and MTs 300, such message services set may include FIN and FileAct). If, for example, a Business Application Model is qualified as being compatible with sets of FIN messaging or FileAct generally, then such sets of FIN message types or FileAct, as the case may be, will be permitted to be paired with the Partner's Business Application Model in order to enable the integrated offering of such Business Application Model and Alliance Cloud.

The Partner must comply at all times with the security and operational requirements relevant to the Business Connect Solution set out and/or contemplated by **Annex 1** (Security and Operational Requirements). Partner understands and confirms that it will be assessed against these requirements through on-site inspections at least every 3 years.

LICENCE FOR ALLIANCE CLOUD, AND SO ON.

The Partner is granted a non-exclusive, personal and non-transferable right to use and procure use of Alliance Cloud for its End Users in accordance with the terms and conditions of the Agreement. The Partner will be provided with a SWIFT quotation pursuant to which it will order the relevant components necessary to provide the Business Connect Solution to End Users. SWIFT will invoice Partner for the rights granted to Partner under this paragraph and Partner will timely pay SWIFT the fees specified or referenced in, and otherwise comply with, **Annex 5** (Fees/Financial Conditions). The relevant components referenced above will include an identifier code, which is a 'test-only' code and is therefore not published in any directory. The Partner is prohibited from sending live messages and from subscribing to any live messaging services for its own purpose or under its own name/technical identifier code. The Partner is only allowed to use this technical identifier code:

- for Test and Training (T&T) messages, but only to itself and to other Partners in a tightly limited and predefined Closed User Group (CUG) for demo and test purposes. The Partner is thus not allowed to send T&T messages to its End Users or any other SWIFT users.
- per any other instructions or directions provided by SWIFT.

Except as deviated from in the Agreement, provision and use of any software or other relevant components referred to above as well as the provision of support services, are governed by SWIFT General Terms and Conditions and the respective applicable SWIFT standard contractual documentation and service descriptions, including the Alliance Cloud service description. Any set-up services package (as well as any other SWIFT professional services) are governed by SWIFT Services Terms and Conditions. Partner must conform to all such contractual documentation.

The Partner acknowledges that it must comply with, when being itself a SWIFT user, and ensure compliance by its End Users with the BIC policy (as available on swift.com). In that respect, SWIFT users are always identified on SWIFT through their own BIC8 and remain fully responsible for all messages sent or received by them through a Partner. The Partner understands in particular that branch codes belong to the institution identified by the corresponding BIC8 and cannot be used to identify a separate legal entity or a third party.

Furthermore, the Partner must immediately inform SWIFT, using the normal support path, about incidents (for example, cyberattacks) that impact or could impact the provision of its services to End Users. Such incidents may include any of the following events:

- events such as security breaches or data breaches
- events that may prevent an End User from meeting its business requirements or obligations
- events that may prevent the Partner from meeting its obligations as defined in any End User service level agreement

The Partner shall share and disclose all information that SWIFT may require for the forensic investigation of such incidents. The Partner must also ensure assistance to End Users and SWIFT to identify, investigate and resolve problems in case of cyber-attack for instance (security or data breaches) or when not able to provide its business obligations to End Users.

QUALIFICATION AND COMPLIANCE OF BUSINESS APPLICATION MODEL

The Partner must qualify its Business Application Model(s) for enabling the Business Connect Solution under this Programme per the technical and functional validation parameters prescribed by SWIFT by selecting a specific business segment for which it wants to determine compatibility with respect to its Business Application Model(s). Upon successful qualification of its Business Application Model(s), the Partner will be able to send and receive messages over the SWIFT network based on the message sets that have been validated during the compatibility validation. Partners testing and validating their Business Application Model(s) compatibility with SWIFT messaging sets under the technical and functional validation parameters prescribed by SWIFT will, upon successful validation, be able to send and receive (for and on behalf of their End Users) certain sets of SWIFT messages (for example, MTs 100 and/or MTs 300, FileAct and/or InterAct) based upon the SWIFT messaging sets with which their Business Application Model(s) have been found to be compatible.

Notwithstanding any compatibility validation in connection with the technical and functional validation parameters prescribed by SWIFT, Partner must assure at all times that it has validated the technical compatibility of its Business Application Model(s) with all relevant aspects of the message types that are included in the messaging sets it will enable over its Business Application Model(s) and that it is monitoring all new SWIFT standards releases and other SWIFT service or product updates/releases/new versions and making appropriate adjustments to its Business Application Model(s) so as to assure that all message types sent or received by End Users over its Business Application Model(s) will flow smoothly and without interruption and without such message types being “NAKed” or impeded or adversely affected in any way due to the Business Application Model(s) not being compatible with such message types.

Partner agrees and acknowledges that SWIFT is not responsible or liable for consequences resulting from (i) Partner’s failure to comply with the immediately preceding paragraph or (ii) technical/operational issues that result from Partner’s inability to adapt, configure and maintain its Business Application Model(s) in a manner that permits smooth, straight-through processing of End Users’ messages and the integrity of such End Users’ messages. Partner will not act in a manner inconsistent with the preceding sentence when dealing or communicating with End Users.

SWIFT reserves the right to limit the message types and/or sets that Partner may use in connection with its Business Application Model(s) in the event that SWIFT (i) concludes in good faith that Partner is not complying with any of its obligations under this Agreement or (ii) receives what it concludes are significant customer complaints from End Users indicating a failure of any Business Application Model(s) to smoothly and properly accommodate any particular message types or sets.

OTHER RESPONSIBILITIES

The Partner shall be responsible for assuring the submission by each of the End Users of an appropriate electronic or paper form (as made available by SWIFT) for each such End User wishing to use Alliance Cloud through the Partner and shall be responsible for informing its End Users of the SWIFT registration procedures. Partner shall also communicate to its End Users the sets of SWIFT messages that are authorised to be sent through Partner and will promptly and appropriately notify End Users attempting to transmit any messages that are not so authorised. The Partner shall also be responsible for providing each of its End Users with the initial guidance to complete its requirement to self-attest against SWIFT's security controls as set out in the SWIFT Customer Security Controls Framework.

It is a condition precedent to the use of Alliance Cloud by an End User that the End User (i) is and remains a duly registered SWIFT user and (ii) accepts, and subscribes to, use of Alliance Cloud per SWIFT General Terms and Conditions and the Alliance Cloud Service Description from time to time in effect. For these governance, operational and security reasons, each of the End Users willing to use Alliance Cloud will be required to complete the above-mentioned paper or electronic form available on swift.com to register as a SWIFT user and confirm acceptance of the applicable terms and conditions.

The Partner will in principle represent its End Users towards SWIFT. However, SWIFT remains the direct contact towards those End Users for all matters relating to SWIFT usership/membership and all matters relating to the proper execution of the intents and purposes of this Agreement. When representing its End Users, the Partner warrants to SWIFT that it has all necessary authority, permissions and capacity to do so, including, without limitation, the authority to have access to, and to communicate with SWIFT regarding, (i) the SWIFT messages End Users send or receive over the SWIFT network and (ii) communications and documents between SWIFT and End Users. The Partner agrees to keep its End Users informed of all acts, orders, and subscriptions performed for them or on their behalf, and advises them of the terms and conditions applicable to them as a result thereof. The Partner will keep its End Users duly and timely informed of all relevant matters concerning their SWIFT messaging and the transmission of such messages over the SWIFT network over the Business Application Model(s). The Partner shall ensure understanding by its End Users of the Business Connect Solution and model.

The Partner acknowledges and agrees that its End Users will also be allowed to use Alliance Cloud to send messages directly on SWIFT (without going through the Partner or using its Business Application Model(s)).

Should the Partner end or change its relationship with one of its End Users in respect to the use of Alliance Cloud or any other SWIFT service or product or in the case of termination of this Agreement by one of the parties, the Partner will promptly notify SWIFT of such change so as to allow SWIFT to revisit the terms of use of Alliance Cloud and/or any other such SWIFT service or product by such End User as needed or as SWIFT considers appropriate.

In the event of termination of this Agreement (i) the parties shall use commercially reasonable efforts to assist affected End Users in finding alternative connectivity to SWIFT and/or alternative configuration of any other affected SWIFT services or products and (ii) SWIFT shall not be responsible for migration costs associated with moving End Users to alternative connectivity to SWIFT or alternative configurations.

AMENDMENT OF LIABILITY CAP REFERENCED IN ARTICLE 11.3

In article 11.3 of the Enabler Terms and Conditions, and strictly with respect to claims of the type described in such article that solely relate to the Business Connect Solution, the referenced amount of "10,000 Eur" is removed and replaced with "100,000 Eur". This separate liability cap is separate from, and cannot be cumulated or stacked with, the liability cap that would apply to claims not related to the Business Connect Solution.

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