THIRD PARTY TERMS

Third Party	Product Function	OneSpan Product	Location	Flow Down Terms
Belgian Mobile ID	Mobile authentication and Qualified Electronic Signature	OneSpan Sign, Secure Agreement Automation, Identity Verification	Belgium	Set forth below
Equifax Canada Co.	Knowledge base authentication services	OneSpan Sign	Canada	Set forth below
Equifax Information Services LLC	Knowledge base authentication services	OneSpan Sign	United States	Set forth below
Mitek Systems, Inc. ("Mitek")	Identity document verification	Secure Agreement Automation (optional)	Europe, United States	Set forth below
Jumio Corporation	Identity document verification	Secure Agreement Automation (optional), Identity Verification (optional)	United States, India, Columbia and such other countries as Jumio may require	Set forth below
SmartComms, LLC	SmartIQ – forms automation	OneSpan Sign	Global	https://onespan.com/smart-iq-usage-terms
SmartComms, LLC	SmartComm-customer communications management	OneSpan Sign	Global	https://onespan.com/smart-comm-usage-terms
Swisscom Trust Services Ltd ("STS")	Qualified Electronic Signature	OneSpan Sign	Switzerland, EU	Set forth below
Telesign	SMS for authentication and notification purposes	OneSpan SaaS products and certain software products	Europe	Set forth below
Twilio Inc.	SMS for authentication and notification purposes	All OneSpan SaaS products	United States	Set forth below

To the extent applicable to Customer's use of the Product, Customer agrees to comply with the following additional terms which form an integral part of the Contract and/or Order Form concluded between Customer and OneSpan:

Belgium Mobile ID (itsme)

Customer obligations

1. Customer will display the itsme® Brand in accordance with Belgian Mobile ID's branding guidelines or
2. instructions,
3. Customer will notify Supplier of any disputes or claims from an End-User concerning an Operation, and,
4. Customer will comply with instructions and guidelines from Belgian Mobile ID regarding the
5. presentation and functioning of the itsme® Services.

Intellectual property rights:

In its capacity as licensee of the itsme® Brand, Supplier grants to the Customer a non-exclusive, non-assignable, non-transferable right (without the right to sub-license) to use, for the duration of the Contract, the itsme® Brand(s) for the sole purpose of the Customer's exercise of its rights or performance of its obligations under the Contract.

The Customer is only allowed to use the itsme® Brand(s) in accordance with Belgian Mobile ID' guidelines and instructions (including the branding guidelines), as may be amended from time to time by Belgian Mobile ID and as notified by Supplier to Customer. The Customer shall not display the itsme® Brand(s) in any manner that could jeopardize the validity, distinctiveness or reputation of the itsme® Brand(s) or that could be detrimental to Belgian Mobile ID or to Belgian Mobile ID' products and services. The Customer shall not, either during the term of the Contract or after termination thereof, (seek to) register or use any trademark, logo, trade name, other distinctive sign or design or other artwork that is identical or similar to or derived from the itsme® Brand. The items® Brand may not be used in connection with any illegal activity, or in connection with any other activity as may be notified by Belgian Mobile ID from time to time. Any and all goodwill associated with the itsme® Brand shall inure to the benefit of Belgian Mobile ID unless otherwise provided.

Definitions

1. "Itsme® Brand(s)" means the word and figurative trademarks which are registered in the Register of the Trade Marks and Design Registration Office of the European Union under filing number 15761752 and 16876187 and in the Register of the Benelux Office for Intellectual Property under number 994231 and 994230 and all names, logos, trade names, logotypes, trade designations, and other designations, symbols, and marks, that Belgian Mobile ID own, manage, license, or otherwise control now or in the future, anywhere in the world, whether registered or not.
2. "End-User" means any user of the itsme® App.
3. "itsme® App" means the Mobile App developed by Belgian Mobile ID.
4. "itsme® Services" means the authentication or Qualified Electronic Service offered by Belgian Mobile ID.
5. "Operation" means any use of the itsme® Services by the End User (Login, Share ID, Approval or Sign)

Equifax Canada Co. (Canada)

1. Equifax Service

1.1 Customer shall enter into an EULA with Equifax Canada Co. ("**Equifax Canada**").

1.2 Service Level Agreement. Customer understands and agrees that the Equifax Services are made available to Customer pursuant to the following Equifax' Service Levels and Performance Standards:

1.2.1 Availability. The Equifax Services will be operational, a minimum of 95% of the time during any thirty (30) day period, exclusive of scheduled down times. A scheduled downtime is an Equifax Service or Equifax Canada Page downtime which occurs during the scheduled maintenance window or is: (a) scheduled with at least three (3) days prior notice; (b) scheduled for off-peak hours; and (c) does not exceed 6 hours at any one time.

1.2.2 Bandwidth. The bandwidth representing the servers' connection to the Internet will be operating at peak capacity no more than 10 minutes in any 24 hour period and at greater than 70% of peak capacity no more than 60 consecutive minutes of any 24 hour period.

1.2.3 Functionality. Equifax Canada will ensure that each transaction posts only a "soft" inquiry to a consumer's credit report such that only the consumer and not a creditor will see the inquiry and a consumer's credit will not be affected as a result of Customer's inquiry. Equifax Canada will ensure that information provided by Customer with respect to a particular consumer will not be used by Equifax Canada to authenticate or verify information in any other Transaction.

1.2.4 Error Resolution. For all Issues related to Equifax Services, Supplier will make all commercially reasonable attempts to facilitate with Equifax Canada the resolution of the condition within a reasonable time frame of Equifax Canada learning of the loss or degradation of the Equifax Service.

1.2.5 Remedies. Customer's sole and exclusive remedy for Supplier or Equifax Canada's failure to meet the Performance Standards of this exhibit is to terminate the Authentication Service in accordance with the applicable cure periods. In such event, Supplier and Equifax Canada shall have no liability whatsoever for damages or otherwise towards Customer.

2. User Information

2.1 Acknowledgment. Customer acknowledges and agrees that:

2.1.1 receipt of the Equifax Services is dependent upon the input of Equifax User Information into the Equifax Software;

2.1.2 in addition to use of Equifax User Information for the purpose of providing the Equifax Services, Equifax retains Equifax User Information for audit purposes and as well, Equifax Canada may de-identify the Equifax User Information to create and use in an aggregate statistical form; and

2.1.3 Equifax Canada may already be in possession of some of the Equifax User Information which Equifax Canada has otherwise collected, already owns or has separately acquired rights to collect, use and disclose such information.

2.2 Compliance and Consent. In respect of the collection, use and disclosure of Equifax User Information, Customer covenants and agrees:

2.2.1 to comply with any applicable laws, including without limitation, all applicable privacy legislation; and

2.2.2 to obtain the appropriate consent from Equifax Users.

3. Representations and Warranties

3.1 Use of Equifax Service. Customer represents and warrants that the Equifax Services will not be used, in whole or in part, as a basis for determining the eligibility of the Equifax User for credit.

3.2 Specific Disclaimer. Customer acknowledges and agrees that the Equifax Services, including without limitation, the results of the scoring, are dependent, in part, upon information entered by the Equifax User, which cannot be controlled. Supplier makes no representation, warranty or guarantee regarding the accuracy, completeness, or reliability of the Equifax Services, including without limitation, the results of the scoring, to the extent that such accuracy, completeness or reliability is related to or dependent upon the accuracy, completeness or reliability of the information entered by the Equifax User and/or the scoring threshold. Supplier also makes no representation, warranty or guarantee of the scoring threshold implemented to verify or validate the identity of the Equifax User. For clarity, the Equifax Services are intended to streamline and increase the security of Customer's authentication processes and in any case, should not solely be relied upon to approve or decline an Equifax User for receipt of products or services.

4. Indemnity and Limitation of Liability

4.1 Customer Indemnity. Customer shall indemnify, defend and hold harmless Supplier, its officer officers, directors, and employees from and against any and all third party claims, damages, loss, liability, cost or expense, including reasonable legal fees ("Claims") to the extent arising as a result of (a) Customer's violation of any applicable law, regulation, rule or judicial or administrative order related to Customer's access and/or use of the Equifax Software and Equifax Services, (b) Customer's misuse, or any modification of the Equifax Software and/or Equifax Services constituting an infringement of a third party's Intellectual Property Rights, (c) an act or omission under this Attachment or (d) any claim made by Customer against Equifax Canada in respect of this Schedule or any of the services Supplier is providing to Customer under this Attachment.

4.2 Limitation. Neither party shall be liable to the other party or any third party for any special, exemplary, punitive, indirect, multiple, incidental nor consequential damages arising out of or in connection with this Attachment whether based in contract, tort (including, without limitation, negligence) or on any other legal or equitable grounds. With respect to any breaches and defaults under this Attachment, in no event will Supplier be liable to Customer in the aggregate amount greater than the fees paid by Customer to Supplier for the Equifax Services during the six (6) month period preceding a claim giving rise to such liability.

5. DEFINITIONS.

"End User License Agreement" or **"EULA"** means the Client Authorization (Service Provider) agreement between Customer and Equifax Canada Co.

"Equifax Services" means the Equifax Canada services purchased by Customer to be delivered in accordance with the terms and conditions outlined in the Contract.

"Equifax Software" means any software, including any functionalities, source codes, objects, documents, procedures and plans, provided by Supplier or Equifax Canada and which is necessary for the Customer or Supplier to communicate with Equifax Canada in order to receive and/or use the Equifax Services. For clarity, no software will be installed directly onto any Customer servers or hardware, but will be delivered to Customer as a service through an HTML application.

"Equifax User" means the individual whose personal information is provided to Customer and/or Equifax Canada for the purpose of delivering the Equifax Services and more specifically, for the purpose of ID proofing the individual.

"Equifax User Information" means any personal information or other data, including without limitation name, address, date of birth, passport number, and social insurance number, about Equifax Users delivered to Customer and Equifax Canada for the purpose of delivering the Equifax Services that is (1) provided Customer or (2) provided by Equifax Users directly.

"Intellectual Property Rights" means copyright, database right, domain names, patents, registered and unregistered design rights, trade secrets, registered and unregistered trademarks, and all other industrial, commercial or intellectual property rights existing in any country and all the rights to apply for the same.

Equifax Information Services LLC (United States)

The knowledge base authentication service help businesses verify the identity of individuals in connection with business transactions initiated by such individuals (each an **"ID Subject"**) based, in part, on information entered by the ID subject (the "**Authentication Services**"). The Authentication Services will be received by Customer through Supplier subject to the following conditions (the "**Equifax US Terms**"):

1. Customer is a valid business, has a true business identity, and is not an adult entertainment service of any kind, business that operates out of an apartment or within a residence, credit counseling firm, credit repair clinic, an online gambling business of

any kind, massage or tattoo service, an individual seeking information for their private use, or a company or individual involved in spiritual counseling.

2. Customer certifies that it will use the Authentication Services exclusively within Customer's own organization for the purpose of verifying the identity of an ID Subject who initiates a business transaction with the Customer and not for any other purpose; and that it will use and ensure that its employees access to the Authentication Services is in accordance with the terms of Contract.

3. Customer acknowledges and agrees that the Authentication Services do not guarantee the identity of the ID Subject, but merely provide a risk assessment regarding the ID Subject's identity that is derived, in part, from information provided by the ID Subject or otherwise collected from an ID Subject's use of the Authentication Services and relayed by Customer to Equifax US ("**ID Subject Content**"); and that in connection with certain Authentication Services; (i) Customer will establish a risk decision threshold above which the ID Subject is verified or authenticated, depending on the applicable Service, and below which the ID Subject is not verified or authenticated ("Risk Decision Threshold") and Equifax US may act as a consultant to review Customer's risk strategies, but Customer, in its sole discretion, will set its Risk Decision Threshold(s); and (ii) that depending upon Customer's Risk Decision Threshold, an ID Subject may be able to successfully pass verification and authentication even though the individual submitting the ID Subject Content is not the actual individual to whom the ID Subject Content pertains.

4. Customer shall not maintain, copy, capture, reproduce, re-use or otherwise retain in any manner the Queries, the ID Subject responses to the Queries ("**Answers**") or the scores, flags and reason codes generated or other information relating to such Queries and Answers provided by the Authentication Services ("**Scores**"); provided, however, that Customer may capture and retain the unique transaction number generated by the Authentication Services with each transaction (each a "**Transaction ID**") solely for the purpose of (i) audit trail; (ii) calculation of the amount of usage of Authentication Services; and (iii) billing. Without limiting the generality of the foregoing, Customer shall not retain or make copies of, and must purge from its system, the Queries and Answers prior to Customer's receipt of any Score relating to such Queries and Answers; and in the event Customer receives the Authentication Services at its call center (or call center maintained by a service provider), Customer shall ensure that the call center operators are unable to retrieve the Queries and Answers after the delivery of the Score by, for example, disabling the use the back button key after the delivery of the Score. In the event that the Authentication Services do not provide a response, the Queries must be purged as expeditiously as possible but in no event longer than thirty (30) minutes after receipt of such Queries.

5. Customer has the right to transmit and authorize the use of ID Subject Content and hereby authorizes the use of ID Subject Content as required to perform the Authentication Services; analyze, enhance or improve the performance of the Authentication Services; and disclose ID Subject Content as required by law or the operation of the Authentication Services. Customer will timely, reliably and accurately relay the Queries, Answers and other ID Subject Content to and from the Authentication Services and the applicable ID Subject.

6. When providing ID Subjects with access to the Authentication Services via the Internet, Customer will adopt, publish, maintain and adhere to a privacy policy and upon request, provide a copy of Customer's privacy policy.

7. Customer will establish and maintain a manual verification process in the event that Customer determines that an ID Subject does not pass the Risk Decision Threshold or Customer receives a flag from the Authentication Services indicating a possible match from a fraud detection database.

8. Customer will not (i) use or access the Authentication Services outside the territorial boundaries of the United States, Canada, and the United States territories of Puerto Rico, Guam, and the Virgin Islands (collectively, the "Permitted Territory"); regardless of whether such use or access is by off-shore Authorized Agents or authorized Service Providers or an off-shore department or division of Customer, or (ii) export or permit the export of the Authentication Services outside of the Permitted Territory. Customer will not share or permit the use of the Authentication Services, in whole or in part, with any third party.

9. Customer agrees that Equifax US may review Customer's practices and procedures including, without limitation, any relevant documentation, to determine Customer's compliance with these Equifax Terms. Customer shall promptly provide Equifax US with copies of all requested documents and records. If Equifax US reasonably believes a compliance issue exists, Equifax US or its designated representative may enter Customer's facilities, upon at least five (5) business days prior written notice and at a mutually agreed upon time, to conduct an on-site assessment of Customer's practices and procedures relating to Customer's request for, and use of, the Authentication Services and Customer's security practices with respect thereto.

10. Customer shall employ decision-making processes appropriate to the nature of the transaction and in accordance with industry standards, and Customer will use the Authentication Services only for the purposes set forth in these Equifax US Terms. Customer is solely responsible for all results of its use of the Authentication Services. TO THE MAXIMUM EXTENT ALLOWABLE BY LAW, ALL AUTHENTICATION SERVICES ARE PROVIDED BY SUPPLIER AND EQUIFAX US ON AN "AS-IS," AS- AVAILABLE BASIS, AND SUPPLIER, EQUIFAX US AND THEIR DATA PROVIDERS AND SUPPLIERS HEREBY DISCLAIM ANY AND ALL PROMISES, REPRESENTATIONS, GUARANTEES, AND WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITH RESPECT TO THE

ACCURACY, COMPLETEN ESS, CURRENTNESS, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, OF THE AUTHENTICATION SERVICES. IN NO EVENT WILL SUPPLIER, EQUIFAX US OR THEIR DATA PROVIDERS AND SUPPLIERS BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY RELATING TO, ARISING OUT OF, OR CAUSED IN WHOLE OR IN PART BY, ITS ACTS OR OMISSIONS, EVEN IF NEGLIGENT, RELATING TO THE AUTHENTICATION SERVICES.

11. Equifax US may, in its sole discretion, deny access to the Authentication Services by certain Customers ("Denied Customer"). Upon such denial, Supplier will not provide the Authentication Services to the Denied Customer. Denied Customer releases Supplier from any and all claims, demands, actions, causes of action, suits, costs, damages, expenses, compensation, penalties, liabilities and obligations of any kind or nature whatsoever arising out of or relating to such denial. Further, Denied Customer covenants not to sue or maintain any claim, cause of action, demand, cross -action, counterclaim, third-party action or other form of pleading against Supplier arising out of or relating to such denial.

Jumio

Customer obligations

1. Supplier and not Jumio Corporation ("Jumio) is the provider of the Jumio services offerings provided through Supplier's Service (the "Jumio Solutions"), and Customer must look solely to Supplier with respect to any warranty, support and maintenance and/or any other issues or claims associated with Customer's use of the Jumio Services;
2. Customer my only use the Jumio Solutions for its internal business purposes;
3. In no event shall Jumio be liable to Customer or any third party for any loss profits, indirect, special, incidental or consequential damages or for interruption of use or loss or corruption of data with respect to Customer's receipt and use of the Jumio Solutions.

Mitek

Personal Data and information (including Data and the identity document images) ("Mitek Data") will be purged and permanently erased from Mitek's systems within ninety (90) days from the date such Mitek Data is provided to Mitek. "Exception" data may be retained by Mitek for an additional ninety (90) days if necessary to ensure the accuracy and functionality of the Subscription Services. "Exception" data is defined as submitted Mitek Data where the expected Mitek Data was not properly extracted or verified by the Service.

SmartCom

Usage Policy (SmartCOMM)

This Usage Policy contains the limitations on Customer's use of the Services and the consequences of exceeding those limitations.

1. Definitions

The following terms shall have the following meanings:

"AWS"	means hosting of the Services on Amazon Web Services located in the U.S.;
"Batch"	means groups of Output submitted to the Services on a batch basis via the batch APIs;
"File Storage"	means input files, output files and log files relating to Batch;
"Final Output"	means Output generated by the Services that is no longer editable via the Services and may be issued by Customer to third parties;
"Generated Document"	means Final Output generated by the Services from a single template design in a single output format;
"Interactive Page"	means a Page which can be only edited by Customer using the Services prior to it being Final Output;
"Interim Output"	means any Output except Final Output;
"Non-Interactive Page" or "On-Demand Page"	means a Page which once created by Customer using the Services cannot be further edited;
"Order Year"	means each twelve (12) month consecutive period beginning from the commencement of the License Term;
"Output"	means a Page created through Customer's use of the Services;
"Overage Unit"	means blocks of 10 Users or 1 million Pages;
"Page"	means each: (i) physical page face/side (or electronic equivalent) conforming to ISO 216 or ANSI/ASME Y14.1 generated or recorded Remotely or (ii) an email, SMS, or XML file generated or recorded Remotely;
"Page Allowance"	means the number of Pages which Customer is authorized to process in an Order Year in consideration of the Annual Fee, all being specified or otherwise referred to in an Order;
"Remote" or "Remotely"	means location of SmartCom owned or controlled infrastructure upon which the SmartCom Technology operates; and
"Storage Allowance"	means the space as specified in an Order which is available on SmartCom's systems for storage of Data.

2. Smart Communications

2.1. Page Allowance
Customer's Page Allowance is stated in the Order. If it is exceeded in any Order Year, SmartCom may charge Overages at a premium of 50% above the list price stated in the Order for sufficient Overage Units to cover the excess Volume. If list price is not stated in the Order, then SmartCom's list price, current at the time of the Overage, shall apply as the basis for the list price.

If during any Order Year the average number of kilobytes per Page comprising the Final Output exceeds 100, then the applicable Volumes shall be deemed to be the number of Pages multiplied by the average number of kilobytes per Page and divided by 100.

2.2. Storage Allowance
Customer's Storage Allowance is 1GB per Tenancy. Additional storage usage will be charged at USD600/GB/Order Year.

2.3. Peak Allowance
Customer is permitted to process up to 200 Pages per minute for each million Pages of Page Allowance. For example, if the Page Allowance is 10 Million Pages, then up to 2,000 Pages per minute are permitted.

Maximum concurrent requests are 1 per million Remote Pages of Page Allowance.

If Customer exceeds the above limits by 100% on any single occasion, or on three or more occasions in a calendar month, SmartCom reserves the right to restrict Customer's throughput to levels set forth herein.

2.4 Interim Output
Non-finalized Interactive Pages are the total number of Interactive Pages that have been created but are not Final Output. At the end of each Order Year, non-finalized Interactive Pages will be deemed Final Output for the purpose of calculating whether the total number of Interactive Pages are within the Page Allowance.

2.5 Migration Studio
Each Page processed by Migration Studio shall be deemed to be a Remote Non-Interactive Page for the purposes of determining if the Volumes exceed the Page Allowance. SmartCom reserves the right to restrict usage of Migration Studio to not more than 5,000 Pages in any twenty-four (24) hour period.

3. Prohibitions
If at any time Customer contravenes any of the prohibitions listed in the Contract, SmartCom may in its sole discretion suspend Customer and/or User access to the Services, and may where possible, provide Customer with notice of such suspension.

Usage Policy (SmartIQ)

This Usage Policy contains the limitations on Customer's use of the Services and the consequences of exceeding those limitations.

1. Definitions
The following terms shall have the following meanings:

"Finalized Transaction"	means each Transaction that is finalized by a User or external invitee executing the submit function of the Services;
"Interim Transaction"	means each Transaction that is not a Finalized Transaction;
"Local" or "Locally"	means locations owned or otherwise controlled by Customer at which Data is processed;
"Order Year"	means each twelve (12) month consecutive period beginning from the commencement of the License Term;
"Overage Unit"	means blocks of ten percent (10%) of the Transaction Allowance;
"Remote" or "Remotely"	means location of SmartCom owned or controlled infrastructure upon which the SmartCom Technology operates;
"Session"	means each instance where a User or external invitee creates or accesses a Transaction;
"SmartIQ External User"	means any User with access to SmartIQ Produce other than a SmartIQ Internal User;
"SmartIQ Internal User"	means a User who is an employee or agent of Customer or its Affiliates granted access to SmartIQ Produce;
"SmartIQ Produce"	means the run-time capability of the SmartIQ Services for the processing of Transactions currently branded as 'Produce';
"SmartIQ Solution"	means SmartCom's solutions branded as 'SmartIQ' as at the Effective Date and as set out in an Order;
"SmartIQ Tenancy"	means a single Tenancy running the SmartIQ Solution;
"Storage Allowance"	means the amount of storage provided in each SmartIQ Tenancy;
"Transaction"	means each instance where a User or external invitee initiates a workflow process or interview process within the SmartIQ Solution, and
"Transaction Allowance"	means the number of Finalized Transactions which Customer is authorized to process in an Order Year in consideration of the Annual Fee, all being specified or otherwise referred to in an Order.

2. SmartIQ

2.1. Transaction Allowance

Customer's Transaction Allowance is stated in the Order. If it is exceeded in any Order Year SmartCom may charge Overages at a premium 50% above the list price stated in the Order for sufficient Overage Units to cover the excess Volume. If list price is not stated in the Order, then SmartCom's list price, current at the time of the Overage, shall apply as the basis for the list price.

2.2. Unfinalized Transactions
At the end of each Order Year, each Interim Transaction shall be deemed a Finalized Transaction for the purposes of determining whether the Volumes exceed the Transaction Allowance.

2.3. Storage Allowance
Customer's Storage Allowance is 5GB per SmartIQ Tenancy. Additional storage usage will be charged at USD600/GB/Order Year.

2.4. Peak Allowance
The total number of Sessions in any twenty-four (24) hour period may not exceed five percent (5%) of the Transaction Allowance. If Customer exceeds the Peak Allowance, SmartCom reserves the right to restrict Customer's throughput to the levels set forth herein.

3. Prohibitions
If at any time Customer contravenes any of the prohibitions listed in the Contract ("**Prohibited Activities**"), SmartCom may in its sole discretion suspend Customer and/or User access to the Services. SmartCom may further treat any Prohibited Activity as an irremediable and material breach, entitling SmartCom to terminate the MSA and Order with immediate effect. For the purposes of this Order, Prohibited Activities shall also include any use of the Services for or in connection with online gaming or gambling, IRC (Internet Relay Chat) or related bot as reasonably determined by SmartCom in its sole discretion.

Swisscom Trust Services Ltd.

These terms and conditions are applicable to all purchases of Swisscom Trust Services Ltd ("STS") Products ("STS Products") from Supplier (the "STS Terms"). Notwithstanding anything to the contrary, the STS Terms take precedence over any conflicting terms.

1. Customer agrees to the applicable STS Product service description ("Product Description") and "STS basic document dated 01.04.2021" at https://trustservices.swisscom.com/en/downloads. Supplier expressly does not promise services more extensive than those defined by STS in the Service Description.
2. Customer shall not assert a contractual claim against STS, Swisscom (Switzerland) LTD or Swisscom IT Services Finance S.E.
3. Orders for STS Products are not valid until STS approves of the order between Supplier and STS.
4. Orders for recurring services shall be concluded for an indefinite term with regard to the continuous obligation contained therein and may be terminated at any time unless otherwise provided, subject to three (3) months' written notice, to take effect at the end of a calendar month. If a minimum contract term has been agreed upon, termination is possible at the earliest at the end of the term. It is also possible to terminate only individual partial services, subject to compliance with the notice period in force in each case.
5. Supplier may terminate the STS Products without notice for good cause. Good cause shall exist in situations including but not limited to the following:
   a) the occurrence of events or circumstances that make continuing the agreed cooperation under the relevant contracts unreasonable for the terminating Party, including but not limited to the persistent serious breach of material contractual duties by the other Party;
   b) the official publication of an application for bankruptcy in respect of the other Party or a moratorium granted to it.
   c) the incomplete payment of an advance payment or of other contractually owed collateral;
   d) failure to comply with the rectification deadlines and failure to rectify any serious non-conformity identified in the context of the certification or trust service (ac-cording to the recognition authority's assessment scheme pursuant to the applicable signature legislation);
   e) any failure on the part of Customer to comply with material obligations set forth in the Service Description or any other obligations that may trigger a liability case for the trust services.

   If a breach of contract can be remedied by a party, the other party must warn such party in writing and grant it a period of 60 calendar days to remedy the breach before declaring the termination.
6. Customer warrants that it is located in Switzerland, the European Union, or the European Economic Area.
7. **Trust service of Swisscom**. The technical provisioning and the operation of the All-in Signing Service is done by Swisscom in Switzerland. Swisscom (Switzerland) Ltd is an accredited provider in Switzerland of certification services in accordance with the Federal Act on Electronic Signatures (ESigA) ZertES and Swisscom IT Services Finance S.E. is an accredited provider in Austria of trust services in accordance with the eIDAS Regulation. Supplier acts as a reseller of Swisscom services to the Customer. In view of the above, the Customer agrees that Supplier may disclose to Swisscom the contents of the AIS Contract as well as personal and technical Customer data for the purpose of the provisioning and operation of the All-in Signing Service, to the extent necessary for the implementation of the commercial and technical aspects between Supplier and Swisscom.

8. **Valid declaration of configuration and acceptance and Swisscom contracts as prerequisites**.

The Customer must provide a written declaration of configuration and acceptance to the provider of the trust service, i.e. to Swisscom (Switzerland) Ltd or Swisscom IT Services Finance S.E. This permits Swisscom to activate the service for the Customer and to make the necessary arrangements for this purpose. Depending upon the type of identification process selected by the Customer, additional contracts may need to be concluded between the Customer and Swisscom (hereafter referred to as "Additional Contracts"), including in particular:

- If using the RA app: an RA agency contract (including provisions concerning data protection).
- If registration authority activity is carried out by the Customer: a contract for the delegation of personal identification (including provisions concerning data protection, based on the Customer's implementation concept).
- If there are other processes agreed upon specifically for the individual Customer: an agreement regarding the process in question, based on the Customer's implementation concept.

This Contract shall be valid subject to the condition precedent of acceptance by Swisscom, on the one hand, of the declaration of configuration and acceptance, and on the other hand, of the Additional Contracts and implementation concepts as required pursuant to applicable regulations:

- Implementation concepts required pursuant to applicable regulations shall be deemed to have been accepted by Swisscom upon its express confirmation either in writing or by email.
- The Additional Contracts required pursuant to applicable regulations are accepted by Swisscom upon its signature thereof.
- The declaration of configuration and acceptance shall be deemed to have been accepted unless it is objected to due to deficiencies within 14 days of its receipt by Swisscom or if following an initial objection due to deficiencies, it is expressly accepted either in writing or by email.

In view of the above, the Customer confirms that it has received the documents applicable to its Subscriber application.

9. Information obligations

Except as prohibited by statutory or contractual confidentiality obligations, each of the parties shall inform the other of any developments, incidents, and findings that may be relevant for the other party in connection with the performance of the contract or for the contractual relationship as a whole.

10. Proprietary and usage rights

Supplier grants to Customer, for use by Customer itself, a non-transferrable, non-exclusive right, which shall be limited to the duration of this Contract, to use the services of Supplier specified in the contracts.

All rights to intellectual property existing or arising at the time of performance of the Contract (copyright, patent rights, know-how, etc.) relating to services of Supplier shall be retained by Supplier or the third party rights holder (such as e.g. Swisscom). Neither is restricted in otherwise exploiting or using this intellectual property, nor is either under any duty to Customer in respect of the same. If the parties have developed intellectual property jointly, they authorise each other permanently to use and exploit these rights independently of each other without restriction, subject to confidentiality obligations. The Customer acknowledges the legal validity of the intellectual property rights of Supplier and of any third parties (such as e.g. Swisscom) regarding the services performed by Supplier and shall take no actions that might impair the value of the same. It shall take all actions within its means to prevent any unauthorised use. This paragraph shall survive the termination of the contracts.

TeleSign

1. "Licensed Data" means the results returned to Client by or on behalf of TeleSign in response to Client submitting Client Data as part of the Services.
2. **Customer obligations**
   a) Customer will comply with, and will ensure that its users ("Customer Uses") will comply with: obligations regarding use of the Telesign services as set out in TeleSign's Acceptable Use Policy for review at https://www.telesign.com/acceptable-use-policy, and with all applicable laws and data privacy laws.
   b) Users' use of the Service may be conditional to Users' consent to terms of use set out by third party telecommunications operators, international aggregator, and/or carriers ("Carrier"), or to the Carriers' consent to Users' use of said third party operators' service. Customer acknowledges that each Carrier may have different regulations, whereupon the Carriers' service terms may be paramount.
3. Customer will reasonably cooperate with TeleSign to confirm Customer's or Users' consent to disclosure of Customer data to Carriers for the limited purpose of enabling the provision of the Service and for TeleSign's compliance with the terms of its agreements with the Carriers.
4. As applicable, Customer authorizes TeleSign to provide its identification information ("Caller ID") to relevant Carriers for the Caller ID Management Service and TeleSign may disclose the Caller ID with respect to a specific subscriber in response to a call.

5. Customer shall provide all Users with any disclosure or explanation required by applicable laws concerning the Customer's use of the Services, and obtain, maintain and secure any necessary consent and authorizations from Users that may be required by applicable laws in order to authorize TeleSign's provision of the Telesign services, or otherwise procure lawful use by the Users of TeleSign services, and cooperate with TeleSign in ensuring lawful processing of User data, including any Personal Data, for the provision of the Telesign services.
6. In its use of the Services, it will: (a) comply with Telesign's Acceptable Use Policy; (b) use the Telesign services and the Licensed Data in compliance with all Applicable laws and applicable data privacy laws.
7. Upon termination of the Service or the Contract, TeleSign may retain, use, and disclose Customer usage data: (a) for the duration of TeleSign's accounting, tax, billing, audit, and compliance purposes; (b) to investigate fraud, spam, or unlawful use of the Telesign services; and/or (c) as required and for the limited duration allowed by applicable law.

Twilio

Customer obligations

1. Customer will comply with Twilio's Acceptable Use Policy located at: https://www.twilio.com/legal/aup;
2. Customer is responsible for ensuring that the phone numbers used for the Twilio services are up to date. Failure to do so will result in failed SMS text messages, for which Customer must pay SMS authentication charges;
3. Customer agrees to provide Supplier and Twilio reasonable cooperation regarding information requests from law enforcement, regulators, or telecommunications providers;
4. Customer instructs Supplier and Twilio to use and disclose Twilio Data to: (a) provide the Services consistent with Twilio's then-current Privacy Policy available at https://www.twilio.com/legal/privacy, including detecting, preventing, and investigating security incidents, fraud, spam, or unlawful use of the Services and (b) respond to any technical problems or Customer queries and ensure the proper working of the Twilio services;
5. Subject to the DPA between Customer and Supplier, Customer agrees that Supplier may grant Twilio a right to retain, use, and disclose Twilio Usage Data: (a) for the duration of Twilio's accounting, tax, billing, audit, and compliance purposes; (b) to investigate fraud, spam, or unlawful use of the Services; and/or (c) as required by applicable Law in accordance with the durations fixed by Law, provided that the retention, use, and disclosure of such Customer Usage Data for the foregoing purposes is subject to the confidentiality obligations as set forth in Customer's agreement with Supplier. Supplier contractually requires that Twilio anonymize or otherwise delete Twilio Usage Data when Twilio no longer requires it for the foregoing purposes;
6. Twilio may retain Twilio Content or any portion thereof if required by applicable law; and
7. If Customer records or monitors telephone calls, SMS messages, or other communications using the Twilio services, then Customer will comply with all applicable laws prior to doing so at all times. Customer must obtain prior consent to record or monitor communications using the Twilio services. Customer agrees to indemnify Supplier in accordance to the indemnification requirements located in the Master Terms for claims arising out of or related to Customer's acts or omissions in connection with recording or monitoring telephone calls, SMS messages, or other communications, whether such claims arise under contract, tort, statute of other legal theory.

Definitions:

a) "Twilio Content" means(a) content exchanged by means of use of the Twilio Services, such as text, message bodies, voice and video media, images, and sound; and (b) data stored on Customer's behalf via the Twilio services such as communication logs.

b) "Twilio Data" means the Users' phone numbers, one-time pass codes, and any other information contained in the authentication SMS text provided as part of the SMS Authentication Component that is processed through the Twilio authentication service.

c) "Twilio Usage Data" means data processed by Twilio for the purposes of transmitting, distributing or exchanging Twilio Content; including data used to trace and identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Twilio Services, and the date, time, duration and the type of communication.