

**Contract
between the
State of Washington
State Board for Community & Technical Colleges
and
Telesign Corporation**

This Contract is made and entered into by and between the Washington State Board for Community & Technical Colleges, hereinafter referred to as the "**AGENCY**", and the below named firm, hereinafter referred to as "**CONTRACTOR**."

**Telesign Corporation
13274 Fiji Way Suite 600**

Marina del Rey, CA 90292

Phone: N/A

FAX: N/A

Email: legal@telesign.com

WA State UBI Number: 603-196-029

PURPOSE

SBCTC requires the services of a telephony services provider capable of delivering SMS and voice call messages for Multi-Factor Authentication (MFA), specifically through integration with Okta via Inline Hooks.

SCOPE OF WORK

- A. Exhibit A, attached hereto and incorporated by reference, contains the *General Terms and Conditions* governing work to be performed under this contract, the nature of the working relationship between the AGENCY and the CONTRACTOR, and specific obligations of both parties.

- B.** The CONTRACTOR will provide services and staff, and otherwise do all things necessary for or incidental to the performance of work, as included in the AGENCY'S Request for Quotations and Qualifications No. SBCTC 2025-RFQQ-001, attached as Exhibit B, and the CONTRACTOR'S proposal dated May 9, 2025, attached as Exhibit C, CONTRACTOR's Service Level Agreement (SLA) is attached as Exhibit E.
- C.** Each Authorized Purchaser will engage CONTRACTOR separately via CONTRACTOR's order form attached as Exhibit D. CONTRACTOR's services provided for each specific Authorized Purchaser will be indicated in each individual order form.

PERIOD OF PERFORMANCE

The period of performance under this contract will be from 8-12-2025, or date of execution, whichever is later, through 6-30-2030. The Parties may extend the Contract by written Amendment.

COMPENSATION

CONTRACTOR'S compensation for services rendered shall be based on the rates listed in the Order. If CONTRACTOR'S providers rates change, CONTRACTOR reserves the right to modify the rates and/or the formulae used to calculate the rates by providing AGENCY with at least thirty (30) days' prior notice of any such changes. Any submission of SMS content that requires splitting into more than one message shall be treated as a separate transaction for each SMS sent or received by CONTRACTOR. Each member of the Washington Institutions of Public Higher Education (WIPHE) (each an "Authorized Purchaser") purchasing consortium shall have the ability to make their own purchases using this Contract and the pricing identified herein:

BILLING PROCEDURES AND PAYMENT

AGENCY will pay CONTRACTOR upon provision of services provided and receipt of properly completed invoices, which shall be submitted to the Contract Manager.

The invoices shall describe and document, to the AGENCY'S satisfaction, a description of the work performed, the progress of the project, and fees. The invoice shall include the contract reference number SC 2025-26-102. If expenses are invoiced, provide a detailed breakdown of each type. A receipt must accompany any single expenses in the amount of \$50.00 or more in order to receive reimbursement.

Payment shall be considered timely if made by the AGENCY within thirty (30) calendar days after receipt of properly completed invoices. Payment shall be sent to the address designated by the CONTRACTOR. In addition to its other remedies, Telesign may charge Client interest at the rate equal to the lesser of

one and one percent (1%) per month or the maximum rate permitted by applicable law on all sums that remain unpaid after the expiration of such period.

The AGENCY may, in its sole discretion, terminate the contract in accordance with the Termination section if the CONTRACTOR fails to satisfactorily comply with any term or condition of this contract.

No payments in advance or in anticipation of services or supplies to be provided under this contract shall be made by the AGENCY.

Billing Disputes

AGENCY shall notify CONTRACTOR of any billing discrepancy in writing and with reasonable detail within thirty (30) days of the invoice date. CONTRACTOR shall respond to any notice of billing discrepancy within thirty (30) days of receipt. CONTRACTOR shall provide supporting data upon request and cooperate fully in resolving the issue. The following documentation is reasonably required to resolve the dispute: (a) Rate Dispute – documentation identifying the period, the appropriate rate, total calls, and currency amount in dispute for each country, as well as documentation detailing the rate agreed upon; or (b) Volume Dispute – the disputing party must provide the billing Party with a hard copy of the type of volume dispute being issued. All volume disputes must be accompanied by a call detail record from the disputing party's call detail records supporting the erroneous calls. CONTRACTOR shall not impose late fees, interest, or service suspension on any amounts under formal, good faith dispute. Services shall remain uninterrupted during the first 30 days of the dispute resolution process. All undisputed amounts must be paid in full by the Due Date, including any disputed amounts that are less than 1% of the total or less than \$1,000 (one thousand United States Dollars). If the disputed amount exceeds 1% of the total charged amount or is more than \$1,000 (one thousand United States Dollars), the disputing party may withhold payment of the disputed amount (for the avoidance of doubt, any undisputed amounts must be paid in full), provided that the disputing party notifies the other party in writing of the amount and reasons for the dispute at the time payment is withheld.

Fraud

AGENCY may fall victim to fraudulent activity, which includes, but is not limited to, traffic that the receiving party reasonably determines as: (i) traffic terminated to repeating interactive voice responses ("IVRs") or recording platforms; (ii) traffic not routed for termination in the country of destination and/or to the owner of the number range; (iii) traffic involving numbers that are unallocated or unassigned at the time of the traffic; (iv) machine-generated, sequential, or simultaneous traffic; (v) traffic that is artificially inflated; and (vi) fraudulent attacks known as International Revenue Share Fraud ("IRSF") (collectively, "Fraud Event"). AGENCY acknowledges and agrees that CONTRACTOR does not actively monitor AGENCY'S account and that a Fraud Event does not relieve AGENCY from being responsible for the requests

and usage of the Services via its credentials. CONTRACTOR shall bear financial responsibility for such charges when arising from security vulnerabilities or failure to detect anomalous usage caused by CONTRACTOR'S gross negligence or breach in its security systems. AGENCY shall pay the invoice submitted by CONTRACTOR in full by the invoice due date. However, AGENCY may dispute the invoice(s) due to the Fraud Event by providing written notice to CONTRACTOR within thirty (30) days after the date of the invoice in question. The notice of dispute must include all necessary documentation related to the Fraud Event, so that CONTRACTOR may inform its downstream suppliers accordingly. Specifically, the Fraud Event notice must include, at a minimum, the following documentation: (i) a local Police (or relevant authority) report detailing the Fraud Event (or an online equivalent), or an FBI report filed at <https://www.ic3.gov/Home/FileComplaint> (for US-based clients); (ii) a letter from the AGENCY stating that they were the victim of the Fraud Event, with a clear and detailed description of the attack, including call traces/CDRs and a detailed count of minutes for each country; and (iii) any other documents that may be requested by CONTRACTOR or its suppliers. The Police, FBI, or equivalent authority report must contain, at a minimum, the following information: (i) date of the Fraud Event; (ii) full name of the victim (or company) that suffered the financial loss; and (iii) the destination and volume of minutes. While CONTRACTOR will make reasonable business efforts to assist AGENCY during the dispute process, CONTRACTOR does not guarantee that the dispute will be successful. CONTRACTOR will notify AGENCY of the outcome of the dispute as soon as practicable after a complete notice of dispute has been submitted. If the dispute is successful, a credit note (or other mutually agreed-upon resolution) will be issued to the AGENCY.

CONTRACT MANAGEMENT

The Contract Manager/POC for each of the parties shall be the contact person for all communications and billings regarding the performance of this contract.

CONTRACTOR Contract Manager/POC Information	AGENCY Contract Manager Information
Connor Mullan Telesign Corporation 13274 Fiji Way Suite 600 Marina del Rey, CA 90292 Phone : () Fax: () Email address: cmullan@telesign.com Copy: legalteam@telesign.com	Kenn Nied Director, Network Services & Information Security Officer SBCTC <u>1500 Jefferson St. SE</u> <u>Olympia, WA 98501</u> Phone: (360) 704-4304 Fax: () Email address: knied@sbctc.edu

ACCESSIBILITY

If applicable to CONTRACTOR'S Services, CONTRACTOR remains committed to ensuring its products are accessible to users with disabilities. If applicable, CONTRACTOR strives for WCAG 2.1 Level A/AA and Section 508 conformance. If applicable and required by applicable law to CONTRACTOR'S Services, regular testing (both internal and by a third party) is conducted to identify conformance issues, with processes in place for timely remediation of accessibility issues that are identified.

INSURANCE

The CONTRACTOR shall provide insurance coverage as set out in this section. The intent of the required insurance is to protect the state should there be any claims, suits, actions, costs, damages or expenses arising from any negligent or intentional act or omission of the CONTRACTOR or subcontractor, or agents of either, while performing under the terms of this contract.

The CONTRACTOR shall provide insurance coverage, which shall be maintained in full force and effect during the term of this contract, as follows:

1. Commercial General Liability Insurance Policy. Provide a Commercial General Liability Insurance Policy, including contractual liability, in adequate quantity to

protect against legal liability arising out of contract activity but no less than \$1,000,000 per occurrence.

Additionally, the CONTRACTOR is responsible for ensuring that any subcontractors provide adequate insurance coverage for the activities arising out of subcontracts.

2. Automobile Liability. In the event that services delivered pursuant to this contract involve the use of vehicles, either owned or unowned by the CONTRACTOR, automobile liability insurance shall be required. The minimum limit for automobile liability is:

\$1,000,000 per occurrence, using a Combined Single Limit for bodily injury and property damage.

3. The insurance required shall be issued by an insurance company/ies authorized to do business within the state of Washington. CONTRACTOR shall give AGENCY sixty (60) calendar days notice of any insurance cancellation. CONTRACTOR shall submit to AGENCY within fifteen (15) calendar days of the contract effective date, a certificate of insurance that outlines the coverage and limits defined in the *Insurance* section. CONTRACTOR shall submit renewal certificates as appropriate and requested in writing during the term of the contract.

ASSURANCES

AGENCY and the CONTRACTOR agree that all activity pursuant to this contract will be in accordance with all the applicable current federal, state and local laws, rules, and regulations.

ORDER OF PRECEDENCE

Each of the exhibits listed below is by this reference hereby incorporated into this contract. In the event of an inconsistency in this contract, the inconsistency shall be resolved by giving precedence in the following order:

1. Applicable federal and state of Washington statutes and regulations
2. Special terms and conditions as contained in this basic contract instrument
3. Exhibit A – General Terms and Conditions
4. Exhibit B – Request for Quotations and Qualifications No. SBCTC 2025-RFQQ-001
5. Exhibit C – Contractor's Proposal dated May 9, 2025
6. Any other provision, term or material incorporated herein by reference or otherwise incorporated

ENTIRE AGREEMENT

This contract, including referenced exhibits, represents all the terms and conditions agreed upon by the parties. No other statements or representations, written or oral, shall be deemed a part hereof.

CONFORMANCE

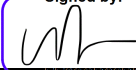
If any provision of this contract violates any statute or rule of law of the state of Washington, it is considered modified to conform to that statute or rule of law.

APPROVAL

This contract shall be subject to the written approval of the AGENCY'S authorized representative and shall not be binding until so approved. The contract may be altered, amended, or waived only by a written amendment executed by both parties.

THIS CONTRACT, consisting of 28 pages and 2 attachment(s), is executed by the persons signing below, who warrant they have the authority to execute the contract.

TELESIGN CORPORATION

Signed by:


EE32CD82DDCC478...

Signature
Chief Legal Officer

8/11/2025

Title

Date

**State of Washington
State Board for Community &
Technical Colleges**



Signature
Executive Director

08/14/2025

Title

Date

**EXHIBIT A -
GENERAL TERMS AND CONDITIONS**

DEFINITIONS

As used throughout this contract, the following terms shall have the meaning set forth below:

- A. "AGENCY" shall mean the Washington State Board for Community & Technical Colleges, any division, section, office, unit or other entity of the AGENCY, or any of the officers or other officials lawfully representing that AGENCY.
- B. "AGENT" shall mean the Director, and/or the delegate authorized to act on the Director's behalf.
- C. "CONTRACTOR" shall mean that firm, provider, organization, individual or other entity performing service(s) under this contract, and shall include all employees of the CONTRACTOR.
- D. "SUBCONTRACTOR" shall mean one not in the employment of the CONTRACTOR, who is performing all or part of those services under this contract under a separate contract with the CONTRACTOR. The terms "SUBCONTRACTOR" and "SUBCONTRACTORS" means SUBCONTRACTOR(s) in any tier.
- E. "Services" means all products offered by CONTRACTOR, now or in the future, as described at <https://www.telesign.com/services> or otherwise provided by CONTRACTOR, and including any Services delivered or accessed via an SDK or the Client Portal (including but not limited to outbound and inbound SMS messages and telephone calls to and from Users). References to "Services" herein shall include Support, as applicable.
- F. "User" For the purposes of this CONTRACT, all Services are intended solely for the internal operational use of AGENCY and its authorized personnel. Any references to "Users" shall mean AGENCY employees, contractors, or other individuals explicitly authorized by AGENCY to receive such Services, and shall not imply that AGENCY is providing services to external customers or third parties.
- G. "AGENCY Data" has the same meaning as "Personal Data" as set out in the Data Processing Addendum.
- H. "Client Portal" means a web portal maintained by CONTRACTOR for all CONTRACTOR's clients where they can securely login using their credentials to access information regarding their CONTRACTOR account such as their billing and recent account activity.

ACCESS TO DATA

CONTRACTOR shall provide access to data generated under this contract to AGENCY at no additional cost, provided that this information is routinely included and part of the services procured by the AGENCY. This includes access to all information that supports the findings, conclusions, and recommendations of the CONTRACTOR'S reports. Computer models, methodology or algorithms used by CONTRACTOR to deliver the services may include proprietary and confidential information and are excluded from the access granted by this provision .

ADVANCE PAYMENTS PROHIBITED

No payments in advance of or in anticipation of goods or services to be provided under this contract shall be made by the AGENCY.

AMENDMENTS

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

This contract may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

AMERICANS WITH DISABILITIES ACT (ADA) OF 1990, PUBLIC LAW 101-336, also referred to as the "ADA" 28 CFR Part 35

The CONTRACTOR must comply with the ADA, which provides comprehensive civil rights protection to individuals with disabilities in the areas of employment, public accommodations, state and local government services, and telecommunications.

ASSIGNMENT

Neither this contract, nor any claim arising under this contract, shall be transferred or assigned by the CONTRACTOR without prior written consent of the AGENCY.

ATTORNEYS' FEES

In the event of litigation or other action brought to enforce contract terms, each party agrees to bear its own attorney fees and costs.

CONFIDENTIALITY/SAFEGUARDING OF INFORMATION

The CONTRACTOR shall not use or disclose any information concerning the AGENCY, or information that may be classified as confidential, for any purpose not directly connected with the administration of this contract, except with prior written consent of the AGENCY, or as may be required by law.

As used herein, "Confidential Information" means all confidential and proprietary information of a Party ("Disclosing Party") disclosed to the other Party ("Receiving Party") that: (a) if disclosed orally is designated as confidential at the time of disclosure, (b) if disclosed in writing is marked as "Confidential" and/or "Proprietary", or (c) reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including, the terms and conditions of this Contract (including pricing and other terms reflected in all Orders) and/or of provision of the Services, screen shots of the Services, pricing in proposals, business and marketing materials, technology and technical information, product designs, and business processes. Confidential Information shall not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (iii) was independently developed by the Receiving Party without breach of any obligation owed to the Disclosing Party, which can be demonstrated with clear and convincing evidence; or (iv) is received from a third party without breach of any obligation owed to the Disclosing Party.

The Receiving Party shall use the same degree of care to protect Confidential Information as it uses to protect its own information of a confidential and proprietary nature, but in no event shall it use less than a commercially reasonable degree of care.

If the Receiving Party is compelled by Applicable Law to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

CONFLICT OF INTEREST

Notwithstanding any determination by the Executive Ethics Board or other tribunal, the AGENCY may, in its sole discretion, by written notice to the CONTRACTOR terminate this contract if it is found after due notice and examination by the AGENT that there is a violation of the Ethics in Public Service Act, Chapter 42.52 RCW; or any similar statute involving the CONTRACTOR in the procurement of, or performance under this contract.

In the event this contract is terminated as provided above, the AGENCY shall be entitled to pursue the same remedies against the CONTRACTOR as it could pursue in the event of a breach of the contract by the CONTRACTOR. The rights and remedies of the AGENCY provided for in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law. The existence of facts upon which the AGENT makes any determination under this clause shall be an issue and may be reviewed as provided in the "Disputes" clause of this contract.

INTELLECTUAL PROPERTY PROVISIONS

Except as expressly set forth herein, CONTRACTOR retains all rights, title, and interest, including all intellectual property rights, in and to the services. This includes, without limitation, all technology, hardware, software, systems, and copies thereof, as well as any upgrades, updates, or modifications. Such intellectual property rights are licensed, not sold, and may be used by AGENCY solely in accordance with the terms of this Contract. All graphics, logos, service marks, and trade names, including third-party names, product names, and brand names associated with each party's products or services (collectively, each party's "Proprietary Marks"), are trademarks of the respective party. Except as set forth in this Contract, neither party may alter, add to, or remove the other party's Proprietary Marks, copyright notices, or other proprietary rights markings from the other party's products or services, nor use the other party's Proprietary Marks without prior, written permission, which may be granted or withheld at the other party's sole discretion.

COVENANT AGAINST CONTINGENT FEES

The CONTRACTOR warrants that no person or selling agent has been employed or retained to solicit or secure this contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, excepting bona fide employees or bona fide established agents maintained by the CONTRACTOR for securing business.

The AGENCY shall have the right, in the event of breach of this clause by the CONTRACTOR, to annul this contract without liability or, in its discretion, to deduct from the contract price or consideration or recover by other means the full amount of such commission, percentage, brokerage or contingent fee.

DISALLOWED COSTS

The Contractor is responsible for any audit exceptions or disallowed costs incurred by its own organization or that of its Subcontractors.

DISPUTES

Except as otherwise provided in this contract, when a dispute arises between the parties and it cannot be resolved by direct negotiation, either party may request a dispute hearing with AGENT.

1. The request for a dispute hearing must:

- Be in writing;
- State the disputed issue(s);
- State the relative positions of the parties;
- State the CONTRACTOR'S name, address, and contract number; and
- Be mailed to the AGENT and the other party's (respondent's) contract manager within 3 working calendar days after the parties agree that they cannot resolve the dispute.

2. The respondent shall send a written answer to the requester's statement to both the agent and the requester within 5 working calendar days.

3. The AGENT shall review the written statements and reply in writing to both parties within 10 working days. The AGENT may extend this period if necessary by notifying the parties.

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

4. The parties agree that this dispute process shall precede any action in a judicial or quasi-judicial tribunal.

Nothing in this contract shall be construed to limit the parties' choice of a mutually acceptable alternate dispute resolution method in addition to the dispute resolution procedure outlined above.

DUPLICATE PAYMENT

The AGENCY shall not pay the CONTRACTOR, if the CONTRACTOR has charged or will charge the State of Washington or any other party under any other contract or agreement, for the same services or expenses.

GOVERNING LAW

This contract shall be construed and interpreted in accordance with the laws of the State of Washington, and the venue of any action brought hereunder shall be in the Superior Court for Thurston County.

CONTRACTOR Warranties.

CONTRACTOR warrants that, for a period of ninety (90) days following delivery, the Services will perform materially as described herein or on <https://www.telesign.com/services>. AGENCY's sole remedy for any breach of this warranty will be, at CONTRACTOR'S option and expense, to either: (a) repair the Service; (b) replace the Service; or (c) terminate this Contract with respect to the defective Service and refund the unused, prepaid rates for the defective Service during the current Term.

AGENCY Warranties.

AGENCY represents and warrants that in its use of the Services, it will: (i) comply with the Acceptable Use Policy available at <https://www.telesign.com/acceptable-use-policy>, (ii) use the Services and the Licensed Data in accordance with all applicable laws, and (iii) obtain and maintain all necessary licenses, consents, and permissions required for CONTRACTOR to perform its obligations under this Contract, including the provision of the Services. "Licensed Data" means the results returned to AGENCY by or on behalf of CONTRACTOR in response to the AGENCY submitting AGENCY Data as part of the Services.

Disclaimers of Warranty.

EXCEPT AS PROVIDED HEREIN, THE SERVICES ARE PROVIDED TO AGENCY "AS IS" AND WITH ALL FAULTS. CONTRACTOR MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, IN CONNECTION WITH THE SERVICES OR ANY HARDWARE OR SOFTWARE USED OR ACCESSED IN CONNECTION WITH THE SERVICES, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. AGENCY ACKNOWLEDGES THAT CONTRACTOR SECURES INFORMATION FROM THIRD-PARTY SOURCES, AND NEITHER CONTRACTOR NOR ITS THIRD-PARTY SOURCES WARRANT THAT THE INFORMATION WILL BE ACCURATE OR ERROR-FREE. CONTRACTOR FURTHER DISCLAIMS ALL WARRANTIES NOT EXPRESSLY SET FORTH HEREIN. AGENCY AGREES THAT CONTRACTOR WILL NOT BE LIABLE FOR ANY CONTENT, INCLUDING BUT NOT LIMITED TO CONTENT THAT IS SENT, RECEIVED, HELD, RELEASED, OR OTHERWISE CONNECTED TO THE SERVICES, CONTENT THAT IS SENT BUT NOT RECEIVED, AND CONTENT SENT USING OR INCLUDED IN THE SERVICES (INCLUDING, WITHOUT LIMITATION, ANY THREATENING, DEFAMATORY, OBSCENE, OFFENSIVE, OR ILLEGAL CONTENT), OR ANY ACCESS TO OR ALTERATION OF CONTENT.

INDEMNIFICATION

To the fullest extent permitted by law, CONTRACTOR shall indemnify, defend, and hold harmless AGENCY and all its officials, agents and employees of AGENCY, from **and** against all third party

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

claims that AGENCY'S authorized use of the Services infringes a copyright, patent, or trademark or misappropriates a trade secret of an unaffiliated third party ("Claim").

In the defense or settlement of any Claim relating to this section, CONTRACTOR may, at its discretion, obtain for AGENCY the right to continue using the Services, replace, or modify the Services so that they become non-infringing, or if such remedies are not reasonably available, terminate this Contract without liability to AGENCY. This Indemnification section sets forth CONTRACTOR'S entire liability and the sole remedy of AGENCY concerning any infringement related to the Services.

If the Services are found to violate the Intellectual Property Rights of a third party, CONTRACTOR will have no obligation under this section for any infringement or violation claim arising as a result of: (i) AGENCY's use of the Services in breach of the Acceptable Use Policy; (ii) the combination, operation, or use of the Services with equipment, software, content, services, or data not supplied or recommended by CONTRACTOR in writing; and/or (iii) AGENCY's failure to use updated or modified software provided by CONTRACTOR to avoid an infringement claim, or failure to install upgrades or patches in a timely manner.

AGENCY's Indemnity. AGENCY will defend CONTRACTOR against any claim brought by an unaffiliated third party arising from: (i) AGENCY's Content and AGENCY Data used with the Services; (ii) AGENCY's use of the Services in breach of this Contract and/or the Acceptable Use Policy; (iii) AGENCY's combination, operation or use of the Services with equipment, software, content, services or data not supplied or recommended by CONTRACTOR in writing.

Limitation of Liability

OTHER THAN IN RESPECT OF ANY INDEMNITY GIVEN, EACH PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY ARISING FROM OR RELATING TO THIS CONTRACT OR THE SUBJECT MATTER HEREOF, UNDER ANY LEGAL THEORY (WHETHER IN CONTRACT, TORT, OR OTHERWISE), WILL IN NO EVENT EXCEED THE TOTAL OF ALL AMOUNTS PAID BY AGENCY TO CONTRACTOR FOR THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE MONTH IN WHICH THE LIABILITY AROSE. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, LOST INCOME, LOST PROFITS, PRESENT AND FUTURE, REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY (EXPRESS OR IMPLIED), ACTIVE OR PASSIVE NEGLIGENCE, INTENTIONAL OR UNINTENTIONAL TORT, STRICT LIABILITY, VIOLATION OF STATUTE, ORDINANCE OR REGULATION, FAILURE OF CONSIDERATION, OR OTHER BASIS, ARISING OUT OF THE PROVISION OF THE SERVICES. NOTWITHSTANDING THE FOREGOING, NEITHER PARTY EXCLUDES OR LIMITS LIABILITY TO THE OTHER PARTY FOR: (I) FRAUD OR FRAUDULENT MISREPRESENTATION; (II) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (III) INTENTIONAL MISCONDUCT OR GROSS NEGLIGENCE; AND/OR (IV) IF SUCH EXCLUSION OR LIMITATION WOULD BE IN BREACH OF ANY APPLICABLE LAW.

INDEPENDENT CAPACITY OF THE CONTRACTOR

The parties intend that an independent contractor relationship will be created by this contract. The CONTRACTOR and his or her employees or agents performing under this contract are not employees or agents of the AGENCY. The CONTRACTOR will not hold himself/herself out as or claim to be an officer or employee of the AGENCY or of the State of Washington by reason hereof, nor will the CONTRACTOR make any claim of right, privilege or benefit that would accrue to such employee under law. Conduct and control of the work will be solely with the CONTRACTOR.

INDUSTRIAL INSURANCE COVERAGE

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

If required by applicable law and AGENCY requests in writing with 60 days notice that the CONTRACTOR shall comply with the provisions of Title 51 RCW, Industrial Insurance, CONTRACTOR will have a right to add the insurance coverage or terminate the Contract immediately upon notice.

LICENSING, ACCREDITATION AND REGISTRATION

The CONTRACTOR shall comply with all applicable local, state, and federal licensing, accreditation and registration requirements/standards, necessary for the performance of this contract.

LIMITATION OF AUTHORITY

Only the AGENT or AGENT'S delegate by writing (delegation to be made prior to action) shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this contract. Furthermore, any alteration, amendment, modification, or waiver or any clause or condition of this contract is not effective or binding unless made in writing and signed by the AGENT.

NONCOMPLIANCE WITH NONDISCRIMINATION LAWS

In the event of the CONTRACTOR'S non-compliance or refusal to comply with any nondiscrimination law, regulation, or policy, this contract may be rescinded, canceled or terminated in whole or in part, and the CONTRACTOR may be declared ineligible for further contracts with the AGENCY. The CONTRACTOR shall, however, be given a reasonable time in which to cure this noncompliance. Any dispute may be resolved in accordance with the "Disputes" procedure set forth herein.

NONDISCRIMINATION

During the performance of this contract, the CONTRACTOR shall comply with all federal and state nondiscrimination laws, regulations and policies.

- a. Nondiscrimination Requirement. During the term of this Contract, CONTRACTOR, including any subcontractor, shall not discriminate on the bases enumerated at RCW 49.60.530(3). In addition, CONTRACTOR, including any subcontractor, shall give written notice of this nondiscrimination requirement to any labor organizations with which CONTRACTOR, or subcontractor, has a collective bargaining or other agreement.
- b. Obligation to Cooperate. CONTRACTOR, including any subcontractor, shall cooperate and comply with any Washington state agency investigation regarding any allegation that CONTRACTOR, including any subcontractor, has engaged in discrimination prohibited by this Contract pursuant to RCW 49.60.530(3).
- c. Default. Notwithstanding any provision to the contrary, AGENCY may suspend CONTRACTOR, including any subcontractor, upon notice of a failure to participate and cooperate with any state agency investigation into alleged discrimination prohibited by this Contract, pursuant to RCW 49.60.530(3). Any such suspension will remain in place until AGENCY receives notification that CONTRACTOR, including any subcontractor, is cooperating with the investigating state agency. In the event CONTRACTOR, or subcontractor, is determined to have engaged in discrimination identified at RCW 49.60.530(3), AGENCY may terminate this Contract in whole or in part, and CONTRACTOR, subcontractor, or both, may be referred for debarment as provided in RCW 39.26.200. CONTRACTOR or subcontractor may be given a reasonable time in which to cure this noncompliance, including implementing conditions consistent with any court-ordered injunctive relief or settlement agreement.
- d. Intentionally omitted

PRIVACY

Personal information including, but not limited to, "Protected Health Information," collected, used, or acquired in connection with this contract shall be protected against unauthorized use, disclosure, modification or loss. CONTRACTOR shall ensure its directors, officers, employees,

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

subcontractors or agents use personal information solely for the purposes of accomplishing the services set forth herein. CONTRACTOR and its subcontractors agree not to release, divulge, publish, transfer, sell or otherwise make known to unauthorized persons personal information without the express written consent of the agency or as otherwise required by law, unless authorized in a Data Processing Agreement in Appendix 1, that has been reviewed and expressly approved in writing by the AGENCY and incorporated by reference into this contract.

Any breach of this provision may result in termination of the contract and the demand for return of all personal information. The CONTRACTOR agrees to indemnify and hold harmless the AGENCY for any damages related to the CONTRACTOR'S unauthorized use of personal information.

PUBLICITY

The CONTRACTOR agrees to submit to the AGENCY all advertising and publicity matters relating to this contract wherein the AGENCY'S name is mentioned or language used from which the connection of the AGENCY'S name may, in the AGENCY'S reasonable judgment, be inferred or implied. The CONTRACTOR agrees not to publish or use such advertising and publicity matters without the prior written consent of the AGENCY.

RECORDS MAINTENANCE

The CONTRACTOR shall maintain books, records, documents, data and other evidence relating to this contract and performance of the services described herein, including but not limited to accounting procedures and practices that sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this contract.

CONTRACTOR shall retain such records for a period of six years following the date of final payment. At no additional cost, these records, including materials generated under the contract, shall be subject at all reasonable times to inspection, review or audit by the AGENCY, personnel duly authorized by the AGENCY, the Office of the State Auditor, and federal and state officials so authorized by law, regulation or agreement.

If any litigation, claim or audit is started before the expiration of the six (6) year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

REGISTRATION WITH DEPARTMENT OF REVENUE

The CONTRACTOR shall complete registration with the Washington State Department of Revenue and be responsible for payment of all taxes due on payments made under this contract.

SAVINGS

In the event funding from state, federal, or other sources is withdrawn, reduced, or limited in any way after the effective date of this contract and prior to normal completion, the AGENCY may terminate the contract under the "Termination for Convenience" clause, without the ten-day notice requirement, subject to renegotiation at the AGENCY'S discretion under those new funding limitations and conditions.

SEVERABILITY

The provisions of this contract are intended to be severable. If any term or provision is illegal or invalid for any reason whatsoever, such illegality or invalidity shall not affect the validity of the remainder of the contract.

SITE SECURITY

While on AGENCY premises, CONTRACTOR, its agents, employees, or subcontractors shall conform in all respects with physical, fire or other security policies or regulations.

SUBCONTRACTING

Neither the CONTRACTOR nor any SUBCONTRACTOR shall enter into subcontracts for any of the work contemplated under this contract without obtaining prior written approval of the AGENCY. This shall not include sub processors mentioned in the DPA. In no event shall the existence of the subcontract operate to release or reduce the liability of the contractor to the Department for any breach in the performance of the contractor's duties. This clause does not include contracts of employment between the contractor and personnel assigned to work under this contract.

Additionally, the CONTRACTOR is responsible for ensuring that all terms, conditions, assurances and certifications set forth in this agreement are carried forward to any subcontracts. CONTRACTOR and its subcontractors agree not to release, divulge, publish, transfer, sell or otherwise make known to unauthorized persons personal information without the express written consent of the agency or as provided by law.

TAXES

All payments accrued because of payroll taxes, unemployment contributions, any other taxes, insurance or other expenses for the CONTRACTOR or its staff shall be the sole responsibility of the CONTRACTOR.

TERMINATION FOR CAUSE

In the event the AGENCY determines the CONTRACTOR has failed to comply with the conditions of this contract in a timely manner, the AGENCY has the right to suspend or terminate this contract. Before suspending or terminating the contract, the AGENCY shall notify the CONTRACTOR in writing of the need to take corrective action. If corrective action is not taken within 30 calendar days, the contract may be terminated or suspended.

The AGENCY reserves the right to suspend all or part of the contract, or prohibit the CONTRACTOR from incurring additional obligations of funds during investigation of the alleged compliance breach and pending corrective action by the CONTRACTOR or a decision by the AGENCY to terminate the contract. A termination shall be deemed a "Termination for Convenience" if it is determined that the CONTRACTOR: (1) was not in default; or (2) failure to perform was outside of his or her control, fault or negligence.

The rights and remedies of the AGENCY provided in this contract are not exclusive and are, in addition to any other rights and remedies, provided by law.

TERMINATION FOR CONVENIENCE

Except as otherwise provided in this contract, either party may, by 30 calendar days written notice, beginning on the second day after the mailing, terminate this contract, in whole or in part. If this contract is so terminated, the AGENCY shall be liable only for payment required under the terms of this contract for services rendered or goods delivered prior to the effective date of termination.

TERMINATION PROCEDURES

Upon termination of this contract, the AGENCY, in addition to any other rights provided in this contract, may require the CONTRACTOR to deliver to the AGENCY any property specifically produced or acquired for the performance of such part of this contract as has been terminated. The provisions of the "Treatment of Assets" clause shall apply in such property transfer.

The termination of this contract shall not release AGENCY from its obligations and liabilities to CONTRACTOR with respect to any rates incurred up to and including the date of termination (whether such rates have been invoiced or not), and any minimum commitments or subscriptions captured in an order form. Any such amounts shall become immediately due and payable upon termination

The rights and remedies of the AGENCY provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this contract.

After receipt of a notice of termination, and except as otherwise directed by the AGENT, the CONTRACTOR shall:

1. Stop work under the contract on the date, and to the extent specified, in the notice;
2. Place no further orders or subcontracts for materials, services, or facilities except as may be necessary for completion of such portion of the work under the contract that is not terminated;
3. Intentionally omitted.

TREATMENT OF ASSETS

- A. Title to all property furnished by the AGENCY shall remain in the AGENCY. Title to all property furnished by the CONTRACTOR, for the cost of which the CONTRACTOR is entitled to be reimbursed as a direct item of cost under this contract, shall pass to and vest in the AGENCY upon delivery of such property by the CONTRACTOR. Title to other property, the cost of which is reimbursable to the CONTRACTOR under this contract, shall pass to and vest in the AGENCY upon (i) issuance for use of such property in the performance of this contract, or (ii) commencement of use of such property in the performance of this contract, or (iii) reimbursement of the cost thereof by the AGENCY in whole or in part, whichever first occurs.
- B. Any property of the AGENCY furnished to the CONTRACTOR shall, unless otherwise provided herein or approved by the AGENCY, be used only for the performance of this contract.
- C. The CONTRACTOR shall be responsible for any loss or damage to property of the AGENCY that results from the negligence of the CONTRACTOR or which results from the failure on the part of the CONTRACTOR to maintain and administer that property in accordance with sound management practices.
- D. If any AGENCY property is lost, destroyed or damaged, the CONTRACTOR shall immediately notify the AGENCY and shall take all reasonable steps to protect the property from further damage.
- E. The CONTRACTOR shall surrender to the AGENCY all property of the AGENCY prior to settlement upon completion, termination or cancellation of this contract
- F. All reference to the CONTRACTOR under this clause shall also include CONTRACTOR'S employees, agents or SUBCONTRACTORS.

U.S. DEPARTMENT OF TREASURY, OFFICE OF FOREIGN ASSETS CONTROL

The agency complies with U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) payment rules. OFAC prohibits financial transactions with individuals or organizations, which have been placed on the OFAC Specially Designated Nationals (SDN) and Blocked Persons sanctions list located at <http://www.treas.gov/offices/enforcement/ofac/index.html>. Compliance with OFAC payment rules ensures that the agency does not conduct business with individuals or organizations that have been determined to be supporters of terrorism and international drug dealing or that pose other dangers to the United States.

Prior to making payment to individuals or organizations, the agency will download the current OFAC SDN file and compare it to agency and statewide vendor files. In the event of a positive match, the agency reserves the right to: (1) make a determination of "reasonability" before taking the positive match to a higher authority, (2) seek assistance from the Washington State Office of the State Treasurer (OST) for advanced assistance in resolving the positive match, (3) comply with an OFAC investigation, if required, and/or (4) if the positive match is substantiated, notify the contractor in writing and terminate the contract according to the Termination for Convenience

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

provision without making payment. The agency will not be liable for any late payment fees or missed discounts that are the result of time required to address the issue of an OFAC match.

WAIVER

Waiver of any default or breach shall not be deemed a waiver of any subsequent default or breach. Any waiver shall not be construed to be a modification of the terms of this contract unless stated to be such in writing and signed by authorized representative of the AGENCY.

USE OF SERVICES & DATA

Acceptable Use Policy. AGENCY shall, and shall ensure that its employees, Agents, contractors, affiliates, and any Users, always abide by CONTRACTOR's Acceptable Use Policy. AGENCY is solely responsible for the payment of all charges for requests submitted from its CONTRACTOR account used to access the Services, and for any damage or other consequences that may result from any misuse of, or inappropriate content transmitted from, AGENCY'S CONTRACTOR account.

SMS Content. Some destination countries of SMS Service have compliance restrictions, policies, or applicable country SMS regulations related to the use case or type of service being provided via a route or provider. In some cases, certain countries may require content whitelisting for specific use cases. Therefore, notwithstanding anything to the contrary in the Contract, all proposed use cases for the SMS Service must first be approved by CONTRACTOR to ensure delivery in those countries. The AGENCY agrees to provide all necessary information regarding the use case for review by CONTRACTOR. In some instances, CONTRACTOR may need to seek additional approval from the respective provider/operator and/or regulatory authorities. The AGENCY will promptly provide and complete all necessary documentation for submission to such provider/operator. Only CONTRACTOR-approved use cases shall be allowed for use with the SMS Service. Any proposed changes by the AGENCY to its previously approved use case must be resubmitted for approval to CONTRACTOR, and if applicable, from the respective provider/operator and/or regulatory authorities. If the proposed use case incurs additional costs not previously covered by the rates, including but not limited to fees or charges imposed by the provider/operator and/or regulatory authorities, CONTRACTOR must advise the AGENCY of such costs prior to incurring them; if the AGENCY agrees to proceed thereafter, the AGENCY agrees to bear the same or reimburse CONTRACTOR accordingly.

Disclosure of Information to third-party Providers/Operators. Notwithstanding anything to the contrary in this contract, AGENCY acknowledges and agrees that CONTRACTOR may be required to disclose AGENCY's or any User's personal information, including but not limited to name, address, email address, and use case, to third-party providers/operators. Such disclosure may occur to set up the Services or when required by the provider/operator to prevent or investigate suspicious activity or Inappropriate Content.

Carrier Consent. AGENCY acknowledges that some results returned to AGENCY by or on behalf of CONTRACTOR in response to the AGENCY submitting AGENCY Data as part of the Services ("Licensed Data") may include data obtained from relevant telecommunications operators and/or carriers (the "Carriers"), and that the use of such CONTRACTOR Services by AGENCY is conditional upon receiving consent from the Carriers. To obtain such consent, AGENCY must complete the AGENCY Onboarding Form, which AGENCY agrees shall be submitted by CONTRACTOR on AGENCY's behalf to the Carriers. AGENCY further consents to CONTRACTOR sharing details of AGENCY's proposed use of such CONTRACTOR Services with the Carriers, which may include AGENCY's Confidential Information, to provide the Carriers with additional context to the information submitted by AGENCY in the AGENCY Onboarding Form. CONTRACTOR hereby certifies that CONTRACTOR will be responsible for the protection of AGENCY Confidential Information and AGENCY Data, including accepting responsibility for the protection of such information while it is in Carriers possession. If the Carriers require

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

AGENCY to update or change its processes, terms of service, usage, or policies as outlined in the AGENCY Onboarding Form, AGENCY agrees to comply with such requirements to obtain consent from the Carriers. AGENCY further agrees that CONTRACTOR shall not be obligated to provide AGENCY with such CONTRACTOR Services until and unless AGENCY has obtained the necessary consent from the Carriers, nor shall AGENCY hold CONTRACTOR liable if the Carriers do not approve the AGENCY's use of such CONTRACTOR Services. In the event that Carriers do not approve AGENCY use of CONTRACTOR Services, CONTRACTOR shall not bill and shall not charge AGENCY for such Services.

Third Party Data Providers. The Licensed Data may include data obtained by third parties such as telecommunications operators. AGENCY hereby consents to the disclosure by CONTRACTOR of AGENCY's (and its Users') identity to such third parties, for the limited purpose of ensuring that CONTRACTOR is complying with the terms of its agreements with such third parties. If any such third party requires Users to provide specific consent to enable the provision of the Services, AGENCY shall reasonably cooperate with CONTRACTOR to confirm the sufficiency of such consent.

APPENDIX 1 – Data Processing Agreement (DPA)

This Data Processing Agreement (“**DPA**”) is made and entered into as of the date of last signature below between **Telesign Corporation**, a California corporation located at 13274 Fiji Way Suite 600, Marina del Rey, CA 90292, USA (“**Telesign**”) and the company specified in the signature block (“**Client**”) (each a “**Party**”, and collectively, the “**Parties**”).

WHEREAS, Telesign is a provider of messaging, mobile identity and fraud prevention services, and the Client has entered into one or several agreement(s) and addenda thereto (the “**Agreement**”) for the Client’s use of the Services (as defined below). In the provision of the Services under the Agreement, Telesign may process certain personal data on behalf of the Client or of Client’s own customers, such data being made available by Client directly or indirectly under the Agreement, and Telesign depending on the Services may also process certain personal data for its own purposes.

NOW, THEREFORE, in consideration of the premises set forth above and the mutual promises, agreements and conditions stated herein, the Parties agree as follows:

1. **Definitions.** Unless the context requires otherwise, the following terms shall have the meaning set out in this

Clause 1:

2.

“**Affiliates**” means a company, person or entity that is owned or controlled by, that owns or controls or is under common ownership or control with a Party. Ownership shall mean direct or indirect ownership of more than 50% of the shares in a company or entity, and control shall mean any power to appoint persons to the board of directors of a company or entity.

“**Applicable Data Protection Law**” shall mean the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 *et seq.* as amended by the California Privacy Rights Act of 2020, Cal. Civil Code § 1798.100 *et seq.* (collectively, “**CCPA**”), Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, “**EU GDPR**”), together with any replacement legislation or any equivalent legislation of any other applicable jurisdiction, the UK Data Protection Act 2018 and UK General Data Protection Regulation (“**UK GDPR**”), the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances as amended from time to time (“**Swiss DPA**”), the Brazilian Lei Geral de Proteção de Dados Pessoais 13.709/2018 (“**LGPD**”), Canadian Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5 (“**PIPEDA**”), Serbian Zakon o zaštiti podataka o ličnosti (“**ZZPL**”), Chinese Personal Information Protection Law (“**PIPL**”), and Singapore Personal Data Protection Act (“**PDPA**”) and all other applicable laws and regulations in any relevant jurisdiction relating to the processing of Personal Data and privacy (such as, without limitation, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as may be amended from time to time).

“**Controller**” means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

“**Data**” means the information exchanged between Parties as described in Annex I attached to this DPA.

“**Data Subject**” means an identified or identifiable natural person whose rights are protected by the Applicable Data Protection Law.

“**Data Subject Rights**” means those rights identified in the Applicable Data Protection Law granted to Data Subjects.

“**Personal Data**” means information that directly or indirectly identifies or relates to a Data Subject.

“**Processor**” means a natural or legal person which processes Personal Data on behalf of the Controller.

“**Restricted Transfer**” means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Data from Switzerland to any other country which is not based on an adequacy decision recognized under the Swiss DPA.

“**Services**” means the Telesign products, solutions, and services (as described at <https://www.telesign.com/services>, including any support services provided in relation thereto) which the Client purchases, accesses or is otherwise permitted to use.

“**Sell**” and “**Share**” shall have the meaning defined in the CCPA.

“**Security Measures**” means the description of the technical and organisational security measures implemented by Telesign in its provision of the Services to Client as set out in Annex II to this DPA.

“**Standard Contractual Clauses**” means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“**EU SCCs**”); (ii) where the UK GDPR applies, the “International Data Transfer Addendum to the EU Commission Standard Contractual Clauses” issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 (“**UK Addendum**”); and (iii) where the Swiss DPA applies, the EU SCC’s with the Swiss additions (“**Swiss SCCs**”).

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

"Sub-processor" means any processor engaged by Telesign who agrees to receive the Personal Data exclusively intended for processing activities to be carried out on behalf of the Client after the transfer in accordance with Client's instructions and in connection with the Agreement for the provision of Services to the Client.

"Supervisory Authority" means an independent public authority pursuant to the Applicable Data Protection Law.

"Third Party" means a natural or legal person other than the Data Subject, Client, Telesign and persons who, under the direct authority of the Client or Telesign, are authorised to process Personal Data.

The terms used in this DPA not defined herein shall have their meanings given in the Applicable Data Protection Law.

2. Processing of Personal Data

- 2.1 Each Party shall fully comply with the obligations that apply to it under the Applicable Data Protection Law. To the extent Telesign acts as an independent Controller of Personal Data that is collected, exchanged, or otherwise Processed in connection with Telesign's performance of the Agreement, Telesign will comply with its Controller obligations under Applicable Data Protection Law, for example by providing notice to Data Subjects, responding to Data Subjects' requests to exercise their rights, as well as identifying a lawful basis of Processing.
- 2.2 To the extent Telesign processes Data as a Processor, on behalf of the Client (or Client's customer) acting as a Controller, in connection with the Agreement, Telesign shall:
 - (a) provide at all times during the performance of this DPA sufficient guarantees for its compliance with the requirements of the Applicable Data Protection Law. Telesign shall not process any Data for purposes other than that which is strictly necessary for the performance of its obligations under the Agreement, and shall only process the Data strictly in accordance with the Client's documented instructions (the **"Permitted Purpose"**) given in this DPA, the Agreement or by any other means during the performance of this DPA. If Telesign is required by any applicable legislation to process any Data otherwise than as permitted herein, Telesign shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Telesign shall immediately inform the Client if, in its opinion, an instruction infringes the Applicable Data Protection Law and shall provide details of the breach or potential breach.
 - (b) treat Data with strict confidence and take all appropriate steps to ensure that disclosure of or access to Data is restricted to its employees, consultants or agents that strictly require such Data to perform the tasks allotted to them by Telesign in the performance of Telesign's obligations under the Agreement (the **"Authorized Persons"**) and excluding all access to Data which are not strictly necessary for the Authorized Persons to perform its part of the Services. Telesign shall ensure that the Authorized Persons who will process Data: (i) are aware of and shall comply with the provisions of this DPA; (ii) are under a duty of confidentiality with respect to the Data no less restrictive than the duties set forth herein prior to any access to the Data. Telesign shall ensure that such confidentiality obligations survive the termination of the employment or contracting agreement; (iii) have received appropriate training in relation to the Applicable Data Protection Law; (iv) are subject to user authentication and log-on processes when accessing the Data; and (v) shall only process the Data as necessary for the Permitted Purpose and in accordance with the Client's instructions.
 - (c) not engage any Sub-processor for the processing of Data without the Client's prior general written authorisation (the **"Approved Sub-processor"**). Notwithstanding this, in the frame of the Parties' relationship as of the date of this Agreement, Client allows Telesign to be assisted by Sub-processors strictly with a view to deliver and improve the agreed Services, provided (i) Telesign shall inform the Client at least 1 calendar month in advance and by means of a written communication about its intention to engage a new Sub-processor, including details on the identity of the Sub-processor, the location where the Data will be processed by such Sub-processor and the concerned data processing activities; (ii) Telesign will enter into written contracts with such Approved Sub-processor guaranteeing at least a level of data protection and information security as provided for herein; and (iii) in any event Telesign will remain fully liable to the Client for any breach of the Approved Sub-processor that is caused by an act, error or omission of the Approved Sub-processor. Client may, within 1 calendar month of Telesign's notification of a new Sub-Processor, object to the appointment of the Sub-processor on reasonable grounds relating to the protection of the Data, in which case the Parties shall then work together promptly and in good faith to resolve the Client's objections and to agree upon a mutually satisfactory solution. The current list of Approved Sub-processors are detailed in Annex III to this DPA.
 - (d) promptly give written notice to and/or shall fully cooperate with the Client if for any reason: (i) Telesign cannot comply, or has not complied, with any portion of this DPA, (ii) it would be in breach of or has breached any Applicable Data Protection Law governing its processing of Data, or (iii) Applicable Data Protection Law no longer allows the lawful transfer of Data from the Client to Telesign. In such cases, Telesign shall take all reasonable, necessary and appropriate steps to remedy any non-compliance, or cease further processing of Data, and the Client may immediately terminate the Agreement and this DPA or access to Data, or take any other necessary action, as determined in its sole discretion.
 - (e) promptly give written notice to and/or shall fully cooperate with the Client to enable the Client to comply with its obligations with regard to the security of the processing of Data, taking into account the nature of the processing and the information available to Telesign.
 - (f) upon becoming aware of any Personal Data breach promptly inform the Client of the Personal Data breach without undue delay and shall provide all such timely information and cooperation as the Client may reasonably require including in order for the Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by Applicable Data Protection Law). Telesign shall further take all such measures and actions as are necessary to remedy

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

or mitigate the effects of the Data breach and shall keep the Client up-to-date about all developments in connection with the Data breach.

- (g) promptly give written notice to and/or shall fully cooperate with the Client in the preparation of any data protection impact assessments performed by the Client, whether on a mandatory or voluntary basis. Telesign shall provide the Client with all such reasonable and timely assistance as the Client may require in order to conduct a data protection impact assessment in relation to the Data and, if necessary, to consult with its relevant data protection authority. Telesign agrees and acknowledges that if the Client receives a request from a data protection authority, the Client may share the terms of this DPA, the Agreement and any other information Telesign provides to demonstrate compliance with this DPA or Applicable Data Protection Law. In addition to the foregoing, if Telesign believes or becomes aware that its processing of the Data is likely to result in a high risk (as defined in the Applicable Data Protection Law, relevant regulatory guidance and case law) with regard to the data protection rights and freedoms of data subjects, it shall promptly inform the Client.

(h) cooperate, at its own expense, as requested by the Client to enable it to respond and comply with (i) the exercise of rights of data subjects pursuant to Applicable Data Protection Law (such as their right of access, right to rectification, right to object to the processing of their Personal Data, right to erasure and right to restrict processing of their Personal Data and their right to data portability) and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulatory authority or any other third party in respect of Data processed by Telesign under this DPA.

(i) promptly inform the Client of any requests relating to the exercise of such rights or complaints, enquiry or correspondence if they are received directly by Telesign and shall provide all details thereof. Furthermore, Telesign shall provide all Data requested by the Client, within a reasonable timescale specified by the Client and shall provide such assistance to the Client to comply with the relevant request within the applicable timeframes. Telesign understands that any response to such direct requests requires prior written authorization from the Client. If necessary, Telesign shall co-operate with the competent Supervisory Authority.

(j) upon the Client's request, to make all such records, appropriate personnel, data processing facilities and any relevant materials available relating to the processing of the Data available to the Client in order to allow the Client to demonstrate compliance with its obligations laid down in the Applicable Data Protection Law. In particular, the Client or a third party appointed by the Client (the "Auditor") may enter Telesign's premises and more specifically the rooms or locations where the Data is processed by Telesign to verify Telesign's compliance hereunder, provided that such inspection shall be carried out with ninety (90) days prior written notice during regular business hours and under a duty of confidentiality. The Client or the Auditor may inspect, audit and copy any relevant records, processes and systems to verify compliance with the Applicable Data Protection Law and this DPA. The Client shall take all reasonable measures to prevent unnecessary disruption to Telesign's operations. The Client will not exercise its inspection rights as set forth in this clause more than once in any twelve (12) calendar month period and with ninety (90) days' prior written notice and such audits shall be conducted at each Party's cost and expense, except (i) if and when required by instruction of a competent Supervisory Authority or (ii) the Client believes a further audit is necessary due to a Personal Data breach suffered by Telesign.

(k) As soon as it is no longer required for the performance of the Services and at the latest upon the expiration or termination of the Agreement, upon Client's request, Telesign shall promptly return or delete all such Data (at the Client's sole election) and any existing copies thereof, at Telesign's sole expense, unless any applicable law requires the further storage of the Data. Telesign shall certify to the Client that all Data has been returned or destroyed in accordance with the foregoing and Client's instructions. If Telesign cannot destroy or delete the Data due to technical reasons, Telesign will immediately inform the Client and will take all appropriate steps to: (i) come to the closest possible to a complete and permanent deletion of the Data and to fully and effectively anonymize the remaining Data; and (ii) make the remaining Data, which is not deleted or effectively anonymized, unavailable for any further processing except to the extent required by any applicable law.

- 2.3 Telesign shall use Data only to provide, maintain, and improve the Services. Data, including any Personal Data therein, may be stored and processed in the United States or any other countries in which Telesign maintains facilities. Client consents to any such transfer and appoints Telesign to conduct such a transfer on Client's behalf in order to provide the Services. Client acknowledges that as part of the Services, for every Transaction, an assessment is carried out as to the fraud risk of a particular Transaction. Client consents to the results of each such Transaction, including the telephone number, IP address, and email related to such Transaction, being re-used by Telesign for the purposes of future fraud identification and prevention as part of the Services, and for purposes of providing the Services to other Telesign customers.
- 2.4 Client shall provide all Data Subjects with any disclosure or explanation required by Applicable Laws concerning the Client's use of the Services, and obtain, maintain and secure any necessary consent and authorizations from Data Subjects that may be required by applicable laws including Applicable Data Protection Law in order to authorize Telesign's provision of the Services, or otherwise ensure a lawful basis for Telesign's provision of the Services and processing of Data, including any Personal Data.

3. International transfers of personal data

- 3.1 Telesign or any Approved Sub-processor shall not make (or permit) a Restricted Transfer of any Personal Data (whether as an exporter or as an importer) unless an adequate level of protection in accordance with the Applicable Data Protection Law is ensured.
- 3.2 The parties agree that when the transfer of Data from Client to Telesign is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:
- (a) **EU GDPR (Controller to Controller)**: in relation to Data that is protected by the EU GDPR where Telesign is a Controller, the EU SCCs will apply completed as follows: (i) Module One will apply; (ii) in Clause 7, the optional docking clause will apply; (iii) in Clause 11, the optional language will not apply; (iv) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Belgian law; (v) in Clause 18(b), disputes shall be resolved before the courts of Belgium; (vi) Annex I of the EU SCCs shall

EXHIBIT A

GENERAL TERMS AND CONDITIONS - GEN

be deemed completed with the information set out in Annex I to this DPA; and (vii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

(b) **EU GDPR (Controller to Processor):** in relation to Data that is protected by the EU GDPR where Telesign is a Processor and Client is the Controller, the EU SCCs will apply completed as follows: (i) Module Two will apply; (ii) in Clause 7, the optional docking clause will apply; (iii) in Clause 9, Option 1 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Clause 2.2(c) of this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Belgian law; (vi) in Clause 18(b), disputes shall be resolved before the courts of Belgium; (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

(c) **EU GDPR (Processor to Processor):** in relation to Data that is protected by the EU GDPR where Telesign is a Sub-processor and Client is a Processor of the Data on behalf of a third party Controller, the EU SCCs will apply completed as follows: (i) Module Three will apply; (ii) in Clause 7, the optional docking clause will apply; (iii) in Clause 9, Option 1 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Clause 2.2(c) of this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Belgian law; (vi) in Clause 18(b), disputes shall be resolved before the courts of Belgium; (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

(d) **UK GDPR:** in relation to Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows: The EU SCCs, completed as set out above in Clause 3.2(a)-(c) of this DPA shall also apply to transfers of such Data; Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above; and the option "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

(e) **Swiss DPA:** In relation Data that is protected by the Swiss DPA, the EU SCCs as implemented in accordance with Clause 3.2(a)-(c) will apply provided that: (i) references in the EU SCCs to "Regulation (EU) 2016/679" or the "GDPR" shall be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" shall be interpreted as references to Switzerland and to Swiss law, as the case may be; (iii) the term 'member state' shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); (iv) the EU SCCs should be interpreted as protecting the data of legal entities until the entry into force of the revised Swiss DPA; (v) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner (FDPIC) and competent courts in Switzerland; and (vi) if the Restricted Transfer is subject to both the Swiss DPA and the GDPR, then a parallel supervision takes place: FDPIC, insofar as the data Restricted Transfer is governed by the Swiss DPA; and the competent EU supervisory authority insofar as the Restricted Transfer is governed by the GDPR (the criteria of Clause 13a for the selection of the competent authority must be observed).

(f) in the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses shall prevail.

4. Security

5.

4.1 Telesign shall implement appropriate and sufficient, technical and organisational security measures prior to and during processing of any Data to protect the security, confidentiality and integrity of the Data and to protect the Data against any form of accidental, unlawful or unauthorized processing. In particular, without limitation, Telesign shall protect the Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, use or access to Data transmitted, stored or otherwise processed and against any form of unlawful processing. Telesign shall ensure a level of security appropriate to the risks presented by the processing of Data and the nature of such Data. Such measures shall include, as appropriate: (i) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (ii) the ability to restore the availability and access to the Data in a timely manner in the event of a physical or technical incident; and (iii) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.2 At a minimum, such measures shall include the organisational and technical measures, which meet or exceed relevant industry practice. These measures shall remain in place throughout the duration that Telesign provides Services to the Client or until Telesign ceases to process Data as a Processor (whichever is later). As of the effective date of the Agreement, Telesign has implemented the Security Measures in Annex II of this DPA. Telesign may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Services.

5. Indemnification

Telesign acknowledges that the obligations set forth in this DPA are essential and that any violation thereof may seriously harm the Client. Telesign shall have full and sole liability for all damages resulting from a failure on its part to comply with the provisions of this DPA. Should any Data Subject to whom the Personal Data relates, a Supervisory Authority, a court or any other regulatory body lodge a claim for compensation against the Client that results from Telesign's breach of its obligations under the Applicable Data Protection Law (a "Claim"), Telesign shall assist and intervene in the Client's defence against such Claim upon the Client's request and shall indemnify and hold harmless the Client against all costs and damages resulting from such Claim. The Client shall give Telesign prompt written notice of any such Claim and shall provide all reasonable cooperation in the defence and settlement of such Claim, at Telesign's expense. The Client shall not make any admission as to Telesign's liability in respect of such a Claim and shall not agree to any settlement in respect of such a Claim without Telesign's written consent.

6. California Consumer Privacy Act

To the extent that CCPA is applicable, except as permitted under the Agreement, this Clause 6 shall take precedence to the extent of any contradictory term otherwise contained herein solely with respect to Processing of Personal Data in the Agreement:

a. To the extent Telesign acts as a "Service Provider" as defined in CCPA Section 1798.140(ag)(1) in addition to the obligations set forth above, Telesign will not (i) Sell or Share Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than for the business purposes specified in the Agreement, including retaining, using, or disclosing it for a commercial purpose other than the business purposes specified in the Agreement or as otherwise permitted under Applicable Data Protection Law; (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Client and Telesign; or (iv) combine it with Personal Data it receives from or

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

on behalf of another entity or that it collects from its own interaction with the Data Subject unless permitted by the CCPA. To the extent required by the CCPA, Telesign certifies that it understands these restrictions and will comply with them.

b. In addition to the obligations set forth in Clause 6a, Telesign will, regardless of its role under the CCPA (i) process Personal Data only for the limited and specified purposes under the Agreement and this DPA; (ii) comply with applicable obligations under the CCPA and provide the same level of privacy protection as is required by the CCPA, (iii) allow Client to take reasonable and appropriate steps to ensure that Telesign uses Personal Data in a manner consistent with Client's obligations under the CCPA; (iv) notify Client if Telesign makes a determination that it can no longer meet its obligations under the CCPA; and (v) allow Client, upon reasonable notice, to stop and remediate Telesign's unauthorized use of Personal Data.

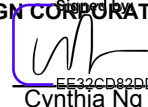
7. General

- 7.1 In the event of a conflict between the provisions of the Agreement, this DPA, and the Standard Contractual Clauses in respect of the processing and protection of Data, the order of precedence is as follows: (1) the Standard Contractual Clauses; (2) this DPA; and (3) the Agreement. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect.
- 7.2 Without prejudice to the provisions of the EU SCCs, UK Addendum and the Swiss SCCs addressing the law which governs them, this DPA shall be governed by and construed in accordance with the laws of the State of California, USA, and the adjudication of any claims or legal disputes arising from or in connection with this DPA shall be held in the courts of the County of Los Angeles, California, USA.
- 7.3 This DPA may from time to time be updated by Telesign to reflect regulatory and compliance changes, Telesign's process enhancements, and similar changes ("DPA Updates") that Telesign deems necessary and advisable. DPA Updates shall be deemed automatically incorporated into and made a part of this DPA upon (i) Telesign's publication of the DPA Updates on its website (at <https://www.telesign.com/dpa>) and (ii) Telesign's notification of the DPA Updates to Client.

CLIENT

By: Joseph M. Humphrey
 Name: Nate Humphrey
 Title: Executive Director
 Date: 08/14/2025

TELESIGN CORPORATION

By: 
 Name: Cynthia Ng
 Title: Chief Legal Officer
 Date: 8/11/2025

Annex I**MODULE ONE: Transfer controller to controller****Categories of data subjects whose personal data is transferred**

- Clients and potential Clients of data exporter
- Employees of data exporter

Categories of personal data transferred

- Clients and potential Clients of data exporter: contact and identity information provided by the data exporter dependent on the Service such as name, address, e-mail address, telephone number and other messaging identifiers, and date of birth; message content provided by the data exporter for transmission such as details of bookings, reservations and appointments, security alerts and one time passcodes; content provided by the data exporter for support and error resolution.
- Employees of data exporter: contact information such as name, email address and phone number; customer login and portal profile information; preferences and settings.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Sensitive data is not processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous basis.

Nature of the processing

- Clients and potential Clients of data exporter: Data exporter will access one or more fraud detection, prevention and communications Services to communicate with the individual and/or evaluate attributes or accuracy of the individual's phone number and other personal details.
- Staff of data exporter: Providing access to the Services.

Purpose(s) of the data transfer and further processing

Data importer may process personal data in accordance with the purposes set out in the Agreement and:

- Clients and potential Clients of data exporter: to provide its Services to the data exporter including obtaining, formatting, cleansing, combining and providing personal data to the Client, and routing messages; to resolve bugs, errors and technical issues including with carriers; to secure the Services; to reconcile bills; to comply with legal, tax, and audit obligations, ensure compliance with Telesign's Acceptable Use Policy, to resolve disputes and meet contractual obligations with carriers; to detect violations of our Agreement;
- Staff of data exporter: to offer, maintain and enhance the Services it or its Affiliates offer; for billing, account and customer relationship purposes (including marketing our Services to staff of the data exporter); to resolve bugs, errors and technical issues; to secure the Services; to comply with legal, tax, and audit obligations, ensure compliance with

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

Telesign's Acceptable Use Policy, resolve disputes and meet contractual obligations with carriers; to detect violations of our Agreement;

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- The duration of the processing is for as long as necessary to enable Telesign's purposes as a controller. The criteria used to determine Telesign's retention periods include: the length of time of Telesign's relationship with data exporter users (for example, the duration of a Telesign customer portal account); whether data exporters modify or their users delete information through their accounts; whether Telesign has a legal or contractual obligation to keep the personal data (for example, certain laws require Telesign to keep records for a certain period of time); whether retention is required by Telesign's legal position (such as in regard to the enforcement of agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation); and whether Telesign needs to retain certain personal data to deliver and improve its Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- In performing its services, data importer will use computing and personnel resources from its processors in the United States, United Kingdom, Serbia, Singapore, Colombia, China and the European Economic Area for the duration needed to perform its obligations under the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

As per the criteria set out in Clause 13(a) of the EU SCCs.

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

- Clients and potential Clients of data exporter
- Employees of data exporter

Categories of personal data transferred

- Clients and potential Clients of data exporter: message content provided by the data exporter for transmission such as details of bookings, reservations and appointments, security alerts and one time passcodes; content provided by the data exporter for support and error resolution.
- Employees of data exporter: contact information such as name, email address and phone number.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Sensitive data is not processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous basis.

Nature of the processing

- Clients and potential Clients of data exporter: Data exporter will access one or more fraud detection, prevention and communications Services to communicate with the individual and/or evaluate attributes or accuracy of the individual's phone number and other personal details.
- Staff of data exporter: Providing access to the Services.

Purpose(s) of the data transfer and further processing

Data importer may process personal data in accordance with the purposes set out in the Agreement and:

- Clients and potential Clients of data exporter: to provide its Services to the data exporter including delivering message content; to resolve bugs, errors and technical issues as requested by data exporter;
- Staff of data exporter: to provide and update the Services as licensed, configured and used by Client and its staff; to resolve bugs, errors and technical issues as requested by data exporter.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- The duration of the processing is limited to the duration needed to perform data importer's obligations under the main Agreement unless a legal obligation applies. The obligations of the data importer with regard to the personal data processing shall in any case continue until the personal data have been properly deleted or have been returned at the request of the data exporter.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- In performing its services, data importer will use computing and personnel resources from its employees, affiliates and sub-processors in the United States, United Kingdom, Serbia, Singapore, Colombia, China and the European Economic Area for the duration needed to perform its obligations under the main Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

As per the criteria set out in Clause 13(a) of the EU SCCs.

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

- Clients and potential Clients of data exporter
- Employees of data exporter

Categories of personal data transferred

- Clients and potential Clients of data exporter: message content provided by the data exporter for transmission such as details of bookings, reservations and appointments, security alerts and one time passcodes; content provided by the data exporter for support and error resolution.
- Employees of data exporter: contact information such as name, email address and phone number.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Sensitive data is not processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous basis.

Nature of the processing

- Clients and potential Clients of data exporter: Data exporter will access one or more fraud detection, prevention and communications Services to communicate with the individual and/or evaluate attributes or accuracy of the individual's phone number and other personal details.
- Staff of data exporter: Providing access to the Services.

Purpose(s) of the data transfer and further processing

Data importer may process personal data in accordance with the purposes set out in the Agreement and:

- Clients and potential Clients of data exporter: to provide its Services to the data exporter including delivering message content; to resolve bugs, errors and technical issues as requested by data exporter;
- Staff of data exporter: to provide and update the Services as licensed, configured and used by Client and its staff; to resolve bugs, errors and technical issues as requested by data exporter.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- The duration of the processing is limited to the duration needed to perform data importer's obligations under the main Agreement unless a legal obligation applies. The obligations of the data importer with regard to the personal data processing shall in any case continue until the personal data have been properly deleted or have been returned at the request of the data exporter.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- In performing its services, data importer will use computing and personnel resources from its employees, affiliates and sub-processors in the United States, United Kingdom, Serbia, Singapore, Colombia, China and the European Economic Area for the duration needed to perform its obligations under the main Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

As per the criteria set out in Clause 13(a) of the EU SCCs.

Annex II

Security Measures

Description of the technical and organisational security measures implemented by Telesign in its provision of the Services to Client:

1. **Security.**
 1. **Security Management System.**
 - a. **Organization.** Telesign designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.
 - b. **Policies.** The data importer's executive management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Client Data. These policies are updated at least once annually.
 - c. **Assessments.** Telesign engages a reputable independent third-party to perform risk assessments of all systems containing Client Data at least once annually.
 - d. **Risk Treatment.** Telesign maintains a formal and effective risk treatment program that includes penetration testing, vulnerability management and patch management to identify and protect against potential threats to the security, integrity or confidentiality of Client Data.
 - e. **Subprocessor Management.** Telesign maintains a formal and effective subprocessor management program.
 - f. **Incident Management.** Telesign reviews security incidents regularly, including effective determination of root cause and corrective action.
 - g. **Standards.** Telesign operates an information security management system that complies with the requirements of ISO/IEC 27001:2013 standard.
 2. **Personnel Security.**
 1. Telesign personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Telesign conducts reasonably appropriate background checks on any employees who will have access to Client Data under this

Agreement, including in relation to employment history and criminal records, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.

2. Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Client Data at all times. Personnel must acknowledge receipt of, and compliance with, Telesign's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Client data are required to complete additional requirements appropriate to their role (e.g., certifications). Telesign's personnel will not process Client data without authorization.

3. **Access and Site Controls.**

1. **Site Controls.**

a. **On-site Data Center Security Operation.** Telesign uses co-location data centers that maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly. All Telesign co-location data centers are ISO 27001 and/or SOC Type 2 certified.

b. **Data Center Access Procedures.** The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

c. **On-site Data Center Security Devices.** Telesign's co-location data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

2. **Access Control.**

a. **Access Management.** Telesign maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Client Data to limit access to Client Data and systems storing, accessing or transmitting Client Data to properly authorized persons having a need for such access. Access reviews are conducted periodically (no less than annually) to ensure that only those personnel with access to Client Data still require it.

b. **Infrastructure Security Personnel.** Telesign has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Telesign's infrastructure security personnel are responsible for the ongoing monitoring of Telesign's security infrastructure, the review of the Services, and for responding to security incidents.

c. **Access Control and Privilege Management.** Telesign's and Client's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized user or administrator.

d. **Internal Data Access Processes and Policies – Access Policy.** Telesign's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Client Data. Telesign designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. Telesign employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Telesign requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Telesign's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity.

4. **Data Center & Network Security.**

1. **Data Centers.**

a. **Infrastructure.** Telesign maintains geographically distributed data centers. Telesign stores all production data in physically secure data centers.

b. **Redundancy.** Infrastructure systems have been designed to minimize single points of failure and the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Telesign to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

EXHIBIT A**GENERAL TERMS AND CONDITIONS - GEN**

- c. **Power.** The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions.
- d. **Server Operating Systems.** Telesign's servers are customized for the application environment and the servers have been hardened for the security of the Services. Telesign employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.
- e. **Disaster Recovery.** Telesign replicates data over multiple systems to help to protect against accidental destruction or loss. Telesign has designed and regularly plans and tests its disaster recovery programs.
- f. **Security Logs.** Telesign's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, Telesign's systems.
- g. **Vulnerability Management.** Telesign performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.
2. **Networks & Transmission.**
- a. **Data Transmission.** Transmissions between data centers are designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Telesign transfers data via Internet standard protocols.
- b. **External Attack Surface.** Telesign employs multiple layers of network devices and intrusion detection to protect its external attack surface. Telesign considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.
- c. **Intrusion Detection.** Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Telesign intrusion detection involves:
- Tightly controlling the size and make-up of Telesign's attack surface through preventative measures;
 - Employing intelligent detection controls at data entry points; and
 - Employing technologies that automatically remedy certain dangerous situations.
- d. **Incident Response.** Telesign maintains incident management policies and procedures, including detailed security incident escalation procedures. Telesign monitors a variety of communication channels for security incidents, and Telesign's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.
- e. **Encryption Technologies.** Telesign makes HTTPS encryption (also referred to as SSL or TLS) available.
5. **Data Storage, Isolation, Authentication and Destruction.** Telesign stores data in a multi-tenant environment on Telesign-controlled servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Telesign logically isolates the data exporter's data from that of other customers of data importer. A central authentication system is used across all Services to increase uniform security of data. The data exporter may choose to make use of certain logging capabilities that Telesign may make available via the Services, products and APIs. Telesign ensures secure disposal of Client Data through the use of a series of data destruction processes.

Annex III**List of Sub-processors**

Company Name	Role	Location	Address
Telesign Belgium BV	Operational support	Belgium	Koning Albert II-laan 27, 1030 Brussels, Belgium
Telesign UK Limited	Operational support (customer services representative)	United Kingdom	2 New Bailey, 6 Stanley Street, Salford, Greater Manchester, M3 5GS
Telesign Singapore Pte. Ltd.	Operational support (customer services representative) for Singapore clients only	Singapore	1 Robinson Road, #17-00, AIA Tower, Singapore (048542)
Telesign (Beijing) Technology Co., Ltd.	Operational support (customer services representative) for China clients only	China	Regus Parkview Green, Floor L15, Beijing, Beijing 100020, China
Telesign Colombia S.A.S.	Operational support (customer services representative)	Colombia	Cr 71 B No. 49 A 27 Sec 2
Telesign d.o.o. Beograd-Novi Beograd	Operational, technical and billing support	Serbia	Tresnjinog cveta 1/IX, 11070 Novi Beograd

EXHIBIT A

GENERAL TERMS AND CONDITIONS - GEN

Adroit Technologies	Operational and technical support	Lithuania	Pylimo st. 41A, LT-01308 Vilnius
Amazon Web Services	Cloud storage	US - North Virginia EU - Ireland	Seattle, WA

Telesign's data centers

Company Name	Role	Hosting Location	Address
Microsoft Corporation	Cloud hosting and storage	- Germany - United States of America	One Microsoft Way, Redmond, WA
Equinix	Data center processing and storage	Netherlands	Equinix AM3, Science Park 610, Amsterdam, 1098XH
Equinix	Data center processing and storage	United States of America	445 N. Douglas St., El Segundo, CA 90245