Introduction

This Data Processing Agreement ("**DPA**") is effective as of the date the Client accepts or begins using the Services governed by this DPA between **Telesign Corporation**, a California corporation located at 13274 Fiji Way Suite 600, Marina del Rey, CA 90292, USA ("**Telesign**") and **PCI-pal (U.K.) limited**, a company incorporated in England and Wales (Registered Number 03960535) and having its registered office at 7 Gamma Terrace, Ransomes Europark, Ipswich, Suffolk, England, IP3 9FF ("**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:

"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 zastiti podataka o licnosti (**"ZZPL"**), Chinese Personal Information Protection Law ("PIPL"), and Singapore Personal Data Protection Act (**"PDPA"**)"), the Digital Operational Resilience Act (Regulation (EU) 2022/2554) ("**DORA**"), Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("**NIS2 Directive**"), 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.

“ICT-related Incident” means any event that has an actual or potential adverse impact on the security, availability, integrity, or continuity of Information and Communication Technology systems used to process Data, including those impacting communication, data storage, or processing services, whether due to internal malfunction or external attack.

“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”**).

“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**").**Where Telesign intends to engage a new Sub-processor** (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. For the avoidance of doubt, Telesign shall not be entitled to engage any Sub-processor for the processing of Data where the Client has objected to the appointment of such Sub-processor on reasonable grounds relating to the protection of the Data and the Parties have been unable to resolve the Client's objection and to agree upon a mutually satisfactory solution. The current list of Approved Sub-processors are detailed in Annex 3 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 Personal 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 or mitigate the effects of the Personal Data Breach and shall keep the Client up-to-date about all developments in connection with the Personal 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, Telesign shall 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, unless such audit is required by instruction of a competent Supervisory Authority or the Client has reasonable grounds to believe that a Personal Data breach has occurred. In all cases, each Party shall bear its own costs and expenses related to the audit.

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.

l. ensure that any sub-processors engaged in the Processing of Data under this Agreement comply with the same incident reporting timelines as required by Telesign under the terms of this Agreement. This includes promptly notifying Telesign

of any security incident or breach affecting the Data, in accordance with the agreed-upon reporting obligations. Telesign shall provide the Client with details of any such incident reported by a sub-processor as soon as reasonably practicable no later than 72 hours after receipt of such notice from the sub-processor, or sooner if required by the Client's own reporting timeline under Applicable Data Protection Law.

m. conduct appropriate due diligence and ongoing third-party risk assessments on all sub-processors, including but not limited to assessments of their technical and organizational security measures, data protection compliance, and operational resilience. Such assessments shall be aligned with applicable regulatory frameworks, including the DORA and the NIS2 Directive, where applicable. Telesign shall maintain records of such assessments and make summaries available to the Client upon reasonable request.

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, UK, EEA, Colombia or Serbia.. Client consents to any such transfer and appoints Telesign to conduct such a transfer on Client's behalf in order to provide the Services. Telesign shall not store or process any Data in any territory outside the United States, UK EEA, Colombia or Serbia without the prior consent of the Client unless the relevant territory ensures an adequate level of protection. 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. Telesign shall also ensure appropriate business continuity measures are in place to maintain data availability and integrity during cross-border incidents that may impact data transfers or accessibility.

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 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

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.

4.3 Telesign shall implement and maintain risk management measures aligned with the DORA conducting regular risk assessments related to the processing of Data, performing impact analyses to evaluate the potential consequences of ICT-related incidents on Data

security and availability, and ensuring continuous monitoring of systems and controls to promptly detect, mitigate, and respond to operational and security risks. In alignment with DORA and NIS2 requirements, Telesign shall classify and report major ICT-related incidents to the relevant authorities and impacted parties within 72 hours of becoming aware of such incidents, based on severity and applicable regulatory thresholds.

4.4 Telesign shall conduct annual Threat-Led Penetration Testing (TLPT), performed by qualified and independent third-party security experts, simulating realistic and targeted cyberattacks to assess the effectiveness of Telesign's security controls and incident response capabilities. The scope of such testing shall include critical systems and infrastructure involved in the Processing of Data. Telesign shall remediate any identified vulnerabilities or weaknesses within a reasonable timeframe based on severity. Upon written request, Telesign shall provide the Client with a high-level summary of the TLPT findings and remediation actions, subject to reasonable confidentiality and security considerations.

4.5 Telesign shall appoint one or more designated security officers responsible for overseeing and ensuring compliance with applicable cybersecurity and operational resilience regulations, including the DORA and the NIS2 Directive. These officers shall coordinate internal security efforts, monitor regulatory developments, and ensure that relevant policies, controls, and response procedures remain aligned with legal and industry obligations.

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:

1. 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 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.
2. 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 unauthorize use of Personal Data.

7. General

7.1 By accessing or using the Services, the Client agrees to the terms of this DPA, which shall form part of and be incorporated into the Agreement between the Client and Telesign. 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 England and Wales**, without regard to any contrary conflict of law principles, and the adjudication of any claims or legal disputes arising from or in connection with this DPA shall be held in the **courts of England**. In the event of a dispute, the Parties shall make reasonable, good-faith efforts to resolve such dispute informally prior to initiating formal proceedings.

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 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, Colombia, 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, , Colombia, 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

- 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.

T**he 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, , Colombia, 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

1. Security Measures

These Security Measures constitute the "Security Measures" referenced in Clause 1 and Clause 4 of this DPA. Description of the technical and organisational security measures implemented by Telesign in its provision of the Services to Client:

Security

1.1. Security Management System.

1. **Organization.** Telesign designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.
2. **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.
3. **Assessments.** Telesign engages a reputable independent third-party to perform risk assessments of all systems containing Client Data at least once annually. All penetration testing and associated assessments shall be conducted in accordance with applicable DORA frameworks, ensuring alignment with regulatory expectations for threat-based testing and operational resilience.
4. **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. The program also incorporates DORA and NIS2-aligned measures such as risk identification, mitigation planning, and continuous monitoring. It further addresses supply chain risks through third-party due diligence, contractual safeguards, and operational resilience planning.
5. **Subprocessor Management**. Telesign maintains a formal and effective subprocessor management program. All third-party providers and subprocessors involved in the processing of Client Data must meet security and operational resilience standards consistent with the requirements of the DORA and the NIS2 Directive, including but not limited to risk management, incident reporting, and business continuity obligations.
6. **Incident Management.** Telesign reviews security incidents regularly, including effective determination of root cause and corrective action.
7. **Standards.** Telesign operates an information security management system that complies with the requirements of ISO/IEC 27001:2013 standard.

2. Personnel Security.

2.1. 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.

2.2. 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

3.1. Site Controls.

1. **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.

2. **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.

3. **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.

3.2. Access Control.

1. **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.

2. **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.

3. **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.

4. **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.

4.1. Data Centers.

1. **Infrastructure.** Telesign maintains geographically distributed data centers. Telesign stores all production data in physically secure data centers.
2. **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.
3. **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.
4. **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.
5. **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. These programs are aligned with applicable regulatory requirements, including the DORA and the NIS2 Directive, to ensure the resilience, continuity, and timely recovery of critical business functions and data. Telesign maintains documented recovery time objectives (RTOs) and recovery point objectives (RPOs), and regularly evaluates recovery capabilities to meet operational and legal obligations under these frameworks.
6. **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.
7. **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.

4.2. Networks & Transmission.

1. **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.

2. **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.
3. **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: (i) Tightly controlling the size and make-up of Telesign's attack surface through preventative measures;(ii) Employing intelligent detection controls at data entry points; and(iii) Employing technologies that automatically remedy certain dangerous situations.
4. **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. Telesign's incident response plan includes early warning notifications to impacted parties where appropriate, ongoing communication throughout the lifecycle of the incident, and final resolution reports detailing the root cause, mitigation steps taken, and actions to prevent recurrence.
5. **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 UK Limited	Operational support (customer services representative)	United Kingdom	2 New Bailey, 6 Stanley Street, Salford, Greater Manchester, M3 5GS
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
Telesign Belgium BV	Operational support	Belgium	Koning Albert II-laan 27, 1030 Brussels, Belgium

Adroiti 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 – USA (Active from July 11, 2025)	One Microsoft Way, Redmond, WA
Equinix	Data center processing and storage	USA (To be decomissioned by July 28, 2025)	1950 North Stemmons Freeway, Suite 1034 Dallas, TX 75207
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
