**CONFIDENTIAL**

# DATA SHARING AGREEMENT

**THIS AGREEMENT** is made on [*date*] (the "**Effective Date**")

**BETWEEN**

(1) **[FULL COMPANY NAME]** a company incorporated in [ ] with offices at [ ] ("**Data Discloser**"); and

(1) **[FULL COMPANY NAME]** a company incorporated in [ ] with offices at [ ] ("**Data Recipient**"),

each a "**Party**" and together, the "**Parties**".

**Background**

(A) The Data Discloser agrees to share the Personal Data with the Data Recipient on terms set out in the Agreement.

(B) The Data Recipient agrees to use the Personal Data on the terms set out in this Agreement.

(C) This is a free-standing Agreement that does not incorporate commercial business terms established by the Parties under separate commercial arrangements.

## 1. Definitions

In this Agreement, unless the context otherwise requires:

(a) "**Affiliate**" means, with respect to each Party, any entity which directly or indirectly controls or is controlled by or is under common control with such Party;

(b) "**Applicable Data Protection Laws**" means (a) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018 ("**DPA**"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications Regulations 2003; (d) California Consumer Privacy Act of 2018 (the "**CCPA**"); and (e) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time;

(c) "**Applicable Laws**" means any of the following, to the extent that it applies to a Party:

(i) any statute, directive, order, enactment, regulation, bylaw, ordinance or subordinate legislation in force from time to time;

(ii) any applicable industry code, policy or standard enforceable by law; and

(iii) any applicable direction, statement of practice, policy, rule or order that is set out by a Regulator that is binding on the Parties;

(d) "**Business Day**" means any day other than a Saturday, Sunday or public holiday in the Parties' relevant jurisdictions;

(e) "**Confidential Information**" means, in respect of a Party or its Representatives:

(i) all confidential information, and information derived from such information in whatever form (including in written, graphic, oral, visual or electronic form), relating to the Party and its Representatives, and customers which is disclosed to the other Party or its Representatives, by the Party or its Representatives or which comes to the other Party's attention in connection with the Project;

(ii) all Personal Data for which one of Parties is responsible under the Applicable Data Protection Laws and which is obtained by the other Party in connection with this Agreement;

(iii) in respect of Data Discloser, all Data Discloser Data;

(iv) the existence and contents of this Agreement; and

(v) all documents that contain or reflect or are generated from any of the foregoing and all copies of any of the foregoing,

in each case whether or not marked confidential;

(f) "**Data Discloser Data**" means data provided to Data Recipient for the purposes of the Project which relates to Data Discloser's subscribers, customers and/or end users, and such subscribers, customer and/or end users' use of Data Discloser's services, as further described in Schedule 1 (*Description of Transfers*)Schedule 1, which may include Data Discloser Personal Data;

(g) "**Data Discloser Personal Data**" means Personal Data for which Data Discloser is responsible under the Applicable Data Protection Laws and which is provided to Data Recipient in connection with this Agreement;

(h) "**Data Protection Authority**" shall mean the relevant data protection authority in the territories where the Parties to this Agreement are established;

(i) "**Data Subject**" shall have the meaning given to this term or equivalent concept in the relevant Applicable Data Protection Laws;

(j) "**Force Majeure Event**" means an act of God, fire, flood, war, act of terrorism, riot, civil commotion, governmental action (excluding regulatory change), labour dispute (save where such dispute involves personnel of the non-performing Party) and any similar event beyond the reasonable control of the non-performing Party;

(k) "**Lawful Export Measure**" means a method allowing for the lawful transfer of Personal Data from a data exporter to a data importer, as may be stipulated by Applicable Data Protection Law or a Regulator from time to time, which may include (depending upon the applicable laws) model transfer terms prescribed by Applicable Data Protection Laws; or prior registration, licensing or permission from a Regulator;

(l) "**Personal Data**" shall have the meaning given in the relevant Applicable Data Protection Laws;

(m) ["**Pre-Approved Subcontractor**" means those entities listed in Schedule 3to this Agreement to which Data Recipient may subcontract its obligations in accordance with Clause 9;]

(n) "**Process**", "**Processed**" or "**Processing**" shall have the meaning given to such terms or equivalent concepts in the relevant Applicable Data Protection Laws;

(o) "**Project**" has the meaning given in the relevant clause;

(p) "**Regulator**" means any supervisory or government agency, body or authority having regulatory or supervisory authority over Data Recipient or Data Discloser, or Data Recipient's or Data Discloser's assets, resources or business, including any Data Protection Authority;

(q) "**Representatives**" means, as applicable in relation to a Party, its directors, officers, employees, agents, consultants, advisers, subcontractors or other representatives and the directors, officers, employees, agents, consultants, advisers, subcontractors or other representatives of each of the Parties.

(r) "**Security Breaches**" has the meaning given to it in Clause 4.1(i)(vii) of this Agreement;

(s) "**Security Documents**" means the relevant documentation, certification, report or equivalent demonstrating compliance with information security requirements under ISO 27001 or other alternative industry standards, including but not limited to SOC1 and SOC2 standards;

(t) "**Special Category Personal Data**" shall have the meaning given to this term or equivalent concept in the relevant Applicable Data Protection Laws;

(u) "**Standard Contractual Clauses**" means, as relevant:

(i) in the case of transfers of Personal Data relating to Data Subjects in the European Economic Area ("**EEA**"), the standard contractual clauses for the transfer of Personal Data to data controllers established in Third Countries set out in the Commission Decision of 4 June 2021 (C(2021) 3972), as amended and restated from time to time;

(ii) in the case of transfers of Personal Data relating to Data Subjects in the United Kingdom, the standard contractual clauses for the transfer of Personal Data to data controllers established in Third Countries set out in the Commission Decision of 27 December 2004 (C(2004) 5271), as amended and restated from time to time; and

(v) "**Third Country**" means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time; and (iii) in relation to Personal Data transfers from any other jurisdiction, any country other than those approved as providing adequate protection for Personal Data by the relevant competent authority of such country from time to time.

1.2 In this Agreement:

(a) the clause and section headings are included for convenience purposes only and shall not affect the interpretation of this Agreement;

(b) any reference to a Party or the Parties includes their successors in interest and permitted assigns;

(c) any reference to "persons" includes natural persons, companies, corporations, partnerships, limited liability companies, firms, associations, organisations, governmental authorities, foundations and trusts (in each case, whether or not having separate legal personality);

(d) any reference to a statute, statutory provision or subordinate legislation shall, except where the context otherwise requires, be construed as referring to such legislation as amended and in force from time to time and to any legislation which re-enacts or consolidates (with or without modification) any such legislation; and

(e) any phrase introduced by the terms "including", "include", "in particular" or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

## 2. Purpose of Data Sharing

2.1 This Agreement sets out the framework for the sharing of Personal Data between the Parties as Data Controllers. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

2.2 The Parties consider this data sharing initiative necessary as [describe reason(s)]. The aim of the data sharing initiative is to [describe aim(s)]. It will serve to benefit [individuals/society] by [describe benefit(s)].

The Parties agree to only process shared Personal Data for the following purposes set out in Schedule 1 (*Description of Transfers*) and the Parties shall not process shared Personal Data in a way that is incompatible with the purposes described in Schedule 1 (*Description of Transfers*) (the "**Project**").

2.3 Each Party shall comply with all appropriate Applicable Data Protection Laws during the Term to the extent relevant to its processing of Personal Data or its obligations under this Agreement.

## 3. Data Discloser Data

3.1 All rights in and to the Data Discloser Data (including any intellectual property rights in and to the Data Discloser Data) are owned by Data Discloser and this Agreement does not transfer any such rights to Data Recipient other than as expressly set out in this Agreement.

3.2 Data Discloser hereby grants Data Recipient and its Representatives a non-exclusive, royalty-free, [worldwide] licence [for the term of this Agreement] to use such Data Discloser Data for the purposes of the Project on and subject to the terms of this Agreement.

3.3 [Data Discloser represents and warrants that it has obtained all necessary consents and complied with all Applicable Laws, including the Applicable Data Protection Laws, in order for Data Recipient to use the Data Discloser Data as contemplated by this Agreement.]

## 4. Protection of Personal Data

4.1 Data Recipient acknowledges and agrees that the Data Discloser Data may include Data Discloser Personal Data. In relation to such Data Discloser Personal Data, Data Recipient shall, and shall procure that its Representatives shall:

(a) use or disclose the Data Discloser Personal Data solely for the purposes of the Project or as otherwise authorised by Data Discloser in writing from time to time;

(b) [store, use and Process the Data Discloser Personal Data on the basis of one or more of the following legal grounds:

(i) [the Data Subject has unambiguously given his or her consent;]

(ii) [the Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;]

(iii) [the Processing is necessary for the purposes of the legitimate interests pursued by the Parties except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child];

(c) [store, use and Process the Data Discloser Personal Data classified as Special Category Personal Data on the basis that the Data Subject has given his explicit consent to the Processing of the shared Special Category Personal Data;]

(d) provide notice to data subject in accordance with Applicable Data Protection Laws;

(e) [store, use and Process the Data Discloser Personal Data in accordance with the transparency requirements under the Applicable Data Protection Laws;]

(f) [store, use or Process the Data Discloser Personal Data for no longer than is necessary to carry out the Project and in any event not longer than any statutory or professional retention periods applicable under any Applicable Data Protection Laws, and shall return or delete any Data Discloser Personal Data once the storage, use or Processing of the relevant Data Discloser Personal Data is no longer necessary for the purposes for which it was originally shared. Data Recipient shall notify Data Discloser within [five (5) Business Days] following the deletion of any Data Discloser Personal Data in accordance with this Clause;]

(g) [not store in or transfer Data Discloser Data to a Third Country, nor allow processing or access to the Data Discloser Personal Data from, a Third Country, other than, in each case, as authorised approved by Data Discloser in writing from time to time;]

(h) [if the Data Recipient Processes the Data Discloser Personal Data for the purposes of direct marketing, the Data Recipient shall ensure that effective procedures are in place to allow the Data Subject to "opt-out" from having their Personal Data used for such direct marketing purposes and the appropriate [explicit] consent has been obtained from the relevant Data Subject to allow the Data Discloser Personal Data to be used for the purposes of direct marketing in compliance with all Applicable Data Protection Laws; and]

(i) to the extent necessary to allow Data Discloser to comply with the Applicable Data Protection Laws:

(i) assist Data Discloser with any subject access requests which it may receive from individuals to whom any Data Discloser Personal Data relates;

(ii) carry out any reasonable request from Data Discloser to amend, transfer or delete any Data Discloser Personal Data;

(iii) [notify Data Discloser [within five (5) Business Days] about any enquiries from the relevant Data Protection Authority in relation to the Data Discloser Personal

Data and cooperate promptly and thoroughly with such Data Protection Authority, to the extent required under the Applicable Data Protection Laws;]

(iv) promptly notify Data Discloser [and in any event within five (5) Business Days] about any legally binding request for disclosure of Data Discloser Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation[. The Data Recipient shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Recipient will provide relevant information about disclosure requests to the Data Discloser, including in relation to its legality review and any challenges to the request];

(v) take adequate technical and organisational measures against unauthorised or unlawful Processing of, accidental loss or destruction of, or damage to, the Data Discloser Personal Data[, including without limitation to:

(A) maintain the security and confidentiality of the Data Discloser Personal Data;

(B) protect against reasonably anticipated threats or hazards to the security or integrity of the Data Discloser Personal Data; and

(C) ensure that those measures continue to provide an adequate level of security;]

(vi) [provide adequate training to its relevant staff and ensure such staff will carry out the security measures and comply with the obligations of Data Recipient under this Agreement;]

(vii) [take appropriate measures to address the Security Breach and notify Data Discloser [within five (5) Business Days] after Data Recipient learns of any misappropriation or unauthorized access to, or disclosure or use of, the Data Discloser Personal Data (collectively, "**Security Breaches**");]

(viii) [investigate each Security Breach that it becomes aware of or has reason to suspect may have occurred [within five (5) Business Days] of becoming aware or having reason to suspect such Security Breach has occurred, and, in the case of an actual Security Breach, provide assistance to Data Discloser in connection with any reasonable investigation that Data Discloser may desire to conduct with respect to such Security Breach;

(ix) implement any steps requested by Data Discloser to limit, stop or otherwise remedy any actual or suspected Security Breach;]

(x) keep appropriate documentation of the Processing it carries out under this Agreement and shall make such documentation available to the Regulator;

(xi) [provide Data Discloser, upon Data Discloser's reasonable request, with a copy of its Security Documents, no more than [twice] annually in order to demonstrate compliance with Data Receiver's obligations under this Agreement, and such Security Documents shall be deemed to satisfy any reporting or audit obligations imposed on Data Receiver under Applicable Data Protection Laws; ]and

(xii) inform Data Discloser if it becomes aware of any Applicable Data Protection Laws that prevent it from fulfilling its obligations under this Clause 4.

4.2 [Data Recipient shall permit Data Discloser at any reasonable time upon [five (5) Business Days'] notice, to be given in writing, to have access to the appropriate part of Data Recipient's premises, systems, equipment, and other materials and data Processing facilities to enable Data Discloser to inspect the same for the purposes of monitoring compliance with Data Recipient's obligations under this Agreement. Such inspection shall not relieve Data Recipient of any of its obligations under this Agreement.]

4.3 In the event that Data Recipient does Process, access and/or store, or permit any third party including its subcontractors to Process, access or store, Personal Data in any Third Country with the consent of the Data Discloser in accordance with Clause 4.1(g), Data Recipient shall, and shall procure that any relevant Affiliate or [third party subcontractor / Pre-Approved Subcontractor] shall:

(a) comply with the data importer's obligations set out in the Standard Contractual Clauses, which are hereby incorporated into and form part of this Agreement (the processing details set out in Schedule 1 (*Description of Transfers*) shall apply for the purposes of Annex 1 and the technical and organisational security measures set out in Schedule 2 (*Technical and Organisational Security Measures*) shall apply for the purposes of Annex 2 to the Standard Contractual Clauses, respectively);

(b) at the Data Discloser's request (from time to time), enter separately into the Standard Contractual Clauses with the relevant Data Discloser or procure that such Affiliate or [third party subcontractor / Pre-Approved Subcontractor] enter into the Standard Contractual Clauses directly with the Data Discloser;

(c) to the extent required by Applicable Data Protection Laws, ensure that such transfer of Personal Data is carried out using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this Agreement); (b) a description of the Processing of Personal Data contemplated under this Agreement; and (c) a description of technical and organisational measures to be implemented by the Data Recipient, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule 1 and the description of technical and organisational measures set out in Schedule 2, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations; and

(d) if agreed between the Data Discloser and Data Recipient, take any other alternative or additional steps reasonably requested by the Data Discloser in order to ensure such Processing takes place in accordance with the requirements of Applicable Data Protection Laws.

## 5. Confidentiality

5.1 Each Party receiving Confidential Information (the "**Recipient Party**") undertakes to the other Party (the "**Disclosing Party**") to:

(a) hold all Confidential Information of the Disclosing Party which it obtains in relation to this Agreement in strict confidence;

(b) not disclose, or authorise the disclosure of, the Disclosing Party's Confidential Information to any third party other than in accordance with Clauses 5.2 and 5.4;

(c) not use, or authorise anyone to use, the Disclosing Party's Confidential Information for any purpose other than the performance of the Recipient Party's obligations or the exercise of its rights or the receipt of any benefits under this Agreement; and

(d) promptly notify the Disclosing Party of any suspected or actual unauthorised use or disclosure of the Disclosing Party's Confidential Information of which the Recipient Party becomes aware and promptly take all reasonable steps that the Disclosing Party may require in order to prevent, stop or remedy the unauthorised use or disclosure.

5.2 Either Party may disclose the other Party's Confidential Information to its Representatives, but only to the extent, and provided, that such persons:

(a) need to know the Confidential Information disclosed to them;

(b) have been informed in writing of the confidential nature of the Confidential Information and the purpose for which it may be lawfully used; and

(c) comply with the terms of this Agreement in respect of the Confidential Information disclosed to them.

5.3 Clause 5.1 shall not apply to Confidential Information to the extent that:

(a) such Confidential Information has been placed in the public domain other than through the fault of the Recipient Party;

(b) such Confidential Information has been independently developed by the Recipient Party without reference to the Confidential Information of the Disclosing Party; or

(c) the Disclosing Party has approved in writing the particular use or disclosure of the Confidential Information.

5.4 Clause 5.1 shall apply to the provision of Security Documents by Data Recipient to Data Discloser.

5.5 Each Party may disclose the other Party's Confidential Information if, and to the extent that, it is required to do so by any governmental authority, court, relevant stock exchange or otherwise by Applicable Law, provided that, to the extent it is permitted to do so, it shall:

(a) notify the other Party as soon as practicable upon becoming aware of the obligation to disclose and, to the extent that it is prevented from notifying the other Party, it shall use all reasonable endeavours to challenge any restriction on disclosure of the request to the other Party, which shall include applying to the court for the removal of such restriction where applicable; and

(b) at the other Party's request, use all reasonable endeavours (where applicable, in cooperation with the other Party) to avoid or limit the disclosure and obtain assurances as to the confidentiality and use of the data from the body to whom the Confidential Information is to be disclosed.

5.6 Neither Party shall, and shall procure that its respective Representatives shall not, issue any press release or other public statement relating to the existence or content of this Agreement, or any information which is disclosed to the other Party as a result of or pursuant to this Agreement without the prior written approval of the other Party.

## 6. Termination

6.1 This Agreement shall commence on the Effective Date and shall remain in full force until it has been terminated in accordance with Clause 6.2 (the "**Term**").

6.2 Either Party may terminate this Agreement:

(a) on [thirty (30) days'] written notice to the other Party; or

(b) immediately by written notice to the other Party:

(i) if the other Party is in material breach of any of its obligations under this Agreement (whether repudiatory in nature or not) and either that breach is incapable of remedy or that Party has failed to remedy that breach within [thirty (30)] days after receiving written notice requiring it to remedy that breach;

(ii) if the other Party is in breach of Applicable Law, including Applicable Data Protection Laws;

(iii) if the other Party suspends, or threatens to suspend, payments or cease business, or is unable to pay its debts as they fall due (or admits such inability), or an order is made, a petition is filed, a notice is given or a resolution passed in connection with the administration, winding-up or dissolution of the other Party, or if any other analogous procedure is taken in any jurisdiction (otherwise than for the purposes of a solvent amalgamation or reconstruction) or an administrative or other receiver, manager, liquidator, administrator, trustee or similar officer is appointed over all or any substantial part of the assets of the other Party or steps are taken to appoint any such officer;

(iv) if the other Party enters into negotiations with or proposes any composition or arrangement with any of its creditors with a view to rescheduling any of its indebtedness or anything analogous to the foregoing occurs in any applicable jurisdiction;

(v) if any expropriation, attachment, sequestration, distress or execution or any analogous process in any jurisdiction affects a substantial part of the assets and is not discharged within [fourteen (14) days]; or

(vi) the other Party is subject either to an enforcement action by any Regulator or ceases to be authorised under any Applicable Law which in either case prevents the other Party from lawfully performing its obligations under this Agreement.

## 7. Consequences of Termination

7.1 [[At any time, on demand in writing by Data Discloser, and in any event] on termination of this Agreement, Data Recipient and each of its Representatives will, within [twenty (20) Business Days]:

(a) destroy or return to Data Discloser (at Data Discloser's sole election) any documents containing Data Discloser Data; and

(b) use all reasonable endeavours to expunge all Data Discloser Data provided to it from any computer, word processor or other device containing Data Discloser Data except any automatically generated back up files, provided that:

(i) Data Recipient's and its Representatives' personnel whose functions are not primarily related to information technology do not access such retained copies; and

(ii) Data Recipient's and its Representatives' personnel whose functions are primarily related to information technology access such copies only as reasonably necessary for the performance of their information technology duties (e.g. for purposes of system recovery).]

7.2 Clauses 2, 4, 5, 8 and 10 shall survive termination of this Agreement.

**8. Limitation of Liability**

8.1 Nothing in this Agreement shall exclude or limit the liability of either Party or its Representatives whether based on an action or claim in contract, tort (including negligence), breach of statutory duty or otherwise arising out of, or in relation to, this Agreement for:

(a) fraud (including fraudulent misrepresentation);

(b) death or personal injury caused by its negligence; or

(c) any other liability which cannot be excluded by Applicable Law.

8.2 [Data Recipient shall indemnify, defend and hold harmless the Data Discloser against any claim, demand, proceeding, action, liability, suit, expense, fine, penalty, damage, loss and cost (including without limitation legal and other professional advisers fees) (each a "**Claim**"), including brought by a Regulator against Data Discloser, to the extent arising out of or in connection with Data Recipient's receipt, use and/or Processing of the Data Recipient Data.] [Data Discloser shall indemnify, defend and hold harmless the Data Recipient against any claim, demand, proceeding, action, liability, suit, expense, fine, penalty, damage, loss and cost (including without limitation legal and other professional advisers fees) (each a "**Claim**"), including brought by a Regulator against Data Recipient, to the extent arising out of or in connection with Data Discloser's failure to comply with this Agreement or Applicable Data Protection Laws.]

8.3 Subject to Clause 8.1 and 8.2, neither Party nor their respective Representatives shall be liable for any indirect or consequential loss arising under or in relation to this Agreement whether as a result of breach of contract, tort (including negligence), breach of statutory duty or otherwise.

8.4 Subject to Clause 8.1 and 8.2, each Party and their respective Representatives' total aggregate liability, whether based on an action or claim in contract, tort (including negligence), breach of statutory duty or otherwise arising out of, or in relation to, this Agreement shall be limited to [*insert appropriate amount*].

8.5 Neither Party shall be liable:

(a) for failure or delay in performing any of its obligations under or pursuant to this Agreement if such failure or delay is due to a Force Majeure Event; or

(b) for a breach of this Agreement to the extent directly caused by the act or omission of the other Party.

**9. Data Recipient Subcontracting**

9.1 [Data Recipient may not subcontract any of its obligations under, or processing activities permitted by, this Agreement without the prior written consent of Data Discloser[, save that it may subcontract its obligations to any Pre-Approved Subcontractor as described in Schedule 3

to this Agreement, including for the purpose of Processing of Data Discloser Data. The Data Receiver shall remain fully responsible to the Data Discloser for the performance of any Pre-Approved Subcontractor's obligations under its contract with the Data Receiver].]

9.2 [Subject to Clause 9.1, if Data Recipient intends to make any changes concerning the addition or replacement of the Pre-Approved Subcontractors in Schedule 3, Data Recipient shall update the list of Pre-Approved Subcontractors on the Data Recipient's applicable web page (or equivalent) at least 30 days before the new Pre-Approved Subcontractor(s) may Process Data Discloser Data, during which time the Data Discloser can object to its appointment or replacement. If Data Discloser does not object in writing within the 30 days, the Data Discloser will be deemed to accept the appointment or replacement of subcontractors and Data Recipient may proceed with the appointment or replacement. If the Data Discloser objects to the appointment or replacement, Data Discloser and Data Recipient shall discuss in good faith Data Discloser's concerns and shall use reasonable efforts to address any of Data Discloser s concerns and, without prejudice to the foregoing, Data Recipient may terminate the Agreement with immediate effect on written notice to the Data Discloser.]

## 10. General

10.1 The rights, powers, privileges and remedies provided in this Agreement are cumulative and are not exclusive of any rights, powers, privileges or remedies provided by law.

10.2 No delay or omission by any Party at any time to require performance of any provision of this Agreement shall affect its right to enforce such provision at a later time. A waiver of any right or remedy under this Agreement shall only be effective if given in writing and shall not be deemed a waiver of any subsequent breach or default.

10.3 No variation or amendment of this Agreement shall be valid unless it is in writing and duly executed by or on behalf of all of the Parties.

10.4 Where any provision of this Agreement is or becomes illegal, invalid or unenforceable in any respect under the laws of any jurisdiction then such provision shall be deemed to be severed from this Agreement and, if possible, replaced with a lawful provision which, as closely as possible, gives effect to the intention of the Parties and, where permissible, that shall not affect or impair the legality, validity or enforceability in that, or any other, jurisdiction of any other provision of this Agreement.

10.5 This Agreement sets out the entire agreement and understanding between the Parties in respect of the subject matter of this Agreement. Each Party acknowledges that it is not relying on, and shall have no remedies in respect of, any undertakings, representations, warranties, promises or assurances (whether made innocently or negligently) that are not set forth in this Agreement. Nothing in this Agreement shall exclude any liability for or remedy in respect of fraud, including fraudulent misrepresentation prior to entering into this Agreement. Except as expressly stated in this Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

10.6 No Party shall assign, transfer, charge or otherwise deal with all or any of its rights under this Agreement nor grant, declare, create or dispose of any right or interest in it without the written consent of the other Party.

10.7 No third party shall have the right to enforce any provision of this Agreement as a third party beneficiary.

10.8 This Agreement may be executed in any number of counterparts. Each counterpart shall constitute an original of this Agreement but all the counterparts together shall constitute but one and the same instrument.

10.9 In the event of a dispute or claim brought by a Data Subject or the Data Protection Authority concerning the processing of Data Discloser Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion. The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Data Protection Authority

10.10 This Agreement and any non-contractual rights or obligations arising out of or in connection with it shall be governed by and construed in accordance with the laws of [ ● ].

10.11 Subject to Clause 10.9, the Parties irrevocably agree that the courts of [ ● ] shall have exclusive jurisdiction to settle any Disputes, and waive any objection to proceedings before such courts on the grounds of venue or on the grounds that such proceedings have been brought in an inappropriate forum. For the purposes of this Clause, "**Dispute**" means any dispute, controversy, claim or difference of whatever nature arising out of, relating to, or having any connection with this Agreement, including a dispute regarding the existence, formation, validity, interpretation, performance or termination of this Agreement or the consequences of its nullity and also including any dispute relating to any non-contractual rights or obligations arising out of, relating to, or having any connection with this Agreement.

[*Signature Page Follows*]

**IN WITNESS WHEREOF** the Parties have caused this Agreement to be executed by their duly authorised representatives as of the date first written above.

Signed by [*name of authorised signatory*]

for and on behalf of

**[FULL COMPANY NAME]** .....

Authorised Signatory

Signed by [*name of authorised signatory*]

for and on behalf of

[**FULL COMPANY NAME**] .....

Authorised Signatory

**SCHEDULE 1**

**DESCRIPTION OF TRANSFERS**

## A. LIST OF PARTIES

**Data exporter(s) – Data Controller:** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

- Name: [*insert details*]
- Address: [*insert details*]
- Contact person's name, position and contact details: [*insert details*]
- Activities relevant to the data transferred under these Clauses: [*insert details*]
- Role (controller/processor): Controller

**Data importer(s) – Data Controller:** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

- Name: [*insert details*]
- Address: [*insert details*]
- Contact person's name, position and contact details: [*insert details*]
- Activities relevant to the data transferred under these Clauses: [*insert details*]
- Role (controller/processor): Controller

## B. Description of Transfer

***Categories of data subjects whose personal data is transferred***

[*To be completed*]

***Categories of personal data transferred***

[*To be completed*]

***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.***

[*To be completed*]

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

[*To be completed*]

***Nature of the processing***

[*To be completed*]

***Purpose(s) of the data transfer and further processing***

[*To be completed*]

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

[*To be completed*]

***For transfers to processors, also specify subject matter, nature and duration of the processing***

[*To be completed if relevant*]

## C. COMPETENT SUPERVISORY AUTHORITY

[*To be completed*]

**SCHEDULE 2**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

Where applicable this Schedule 2 also forms part of the Standard Contractual Clauses.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*For transfers to processors, also describe the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller and, for transfers from a processor to a processor, to the data exporter*

**1. Airwallex**

[Airwallex to insert]

**2. Partner/non-AWX Entity**

| **Technical / Organisational Measure** |
|---|
| **1. Physical Access Control** |
| Data importer shall take, among others, the following technical and organizational measures in order to establish the identity of the authorized persons and prevent unauthorized access to data importer's premises and facilities in which personal data is processed: |
| ☐ All entrances are locked and can only be accessed with the appropriate key / chip card |
| ☐ Windows and doors are protected by an alarm system |
| ☐ All visitors are required to present identification and are signed in by authorized staff |
| ☐ Video monitoring of visitors |
| ☐ Visitors are accompanied by data importer's personnel at all times |
| ☐ Full perimeter and interior surveillance cameras |
| ☐ Use of motion detectors to monitor sensitive areas |
| ☐ Trained security guards are stationed in and around the building 24x7 |
| ☐ Co-location facility - separate locked server suites with card readers |
| ☐ Other measures: _____ |
| 2. System Entry Control |
| Data importer shall take, among others, the following technical and organizational measures in order to prevent unauthorized access to the data processing systems: |
| ☐ Unique user authentication via user name and password for each network and system access required (default passwords changed at 1st login) |
| ☐ Use of state-of-the-art anti-virus software that includes e-mail filtering and malware detection |
| ☐ Use of firewalls |
| ☐ During idle times, user and administrator PCs are automatically locked |
| ☐ User passwords are changed at least every 90 days and only allow complex passwords |
| ☐ Concept of least privilege, allowing only the necessary access for users to accomplish their job function. Access above these least privileges requires appropriate authorization |
| ☐ Starter, mover & leaver housekeeping processes in place which covers role-based access rights |
| ☐ IT access privileges are reviewed regularly (at least every quarter) by appropriate personnel |
| ☐ RSA 2-factor authentication in place for remote connections |
| ☐ Network monitoring services in place 24 x 7 x 365 to detect unauthorized activities |
| ☐ Vulnerability scanning and remediation in place |
| ☐ Data centre and website penetration testing programme in place |

| |
|---|
| ☐ Other measures: _____ |
| 3. Data Access Control |
| Data importer shall take, among others, the following technical and organizational measures in order to prevent unauthorized activities in the data processing systems outside the scope of any granted authorizations: |
| ☐ User and administrator access to the network is based on a role based access rights model. There is an authorization concept in place that grants access rights to data only on a "need to know" basis |
| ☐ Administration of user rights through system administrators |
| ☐ Number of administrators is reduced to the absolute minimum |
| ☐ IT governance & controls audits undertaken annually by external 3rd party |
| ☐ Internal control audits undertaken regularly |
| ☐ Network monitoring services in place 24 x 7 x 365 to detect unauthorized activities |
| ☐ Other measures: _____ |
| 4. Data Transfer Control |
| Data importer shall take, among others, the following technical and organizational measures in order to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons under their electronic transmission or during their transport or recording on data carriers and to guarantee that it is possible to examine and establish where personal data are or have had to be transmitted by data transmission equipment: |
| ☐ Remote access (including during remote maintenance or service procedures) to the IT systems only via VPN tunnels or other state-of-the-art secure, encrypted connections |
| ☐ Use of e-mail encryption |
| ☐ Data transferred by data importer is transported and saved in encrypted form. The relevant areas of the data carriers are encrypted using data and hard drive encryption software |
| ☐ Data storage devices and paper documents are locked away when not in use (clean desk policy) |
| ☐ Physical transports are only performed with locked containers and/or guarded vehicles |
| ☐ Use of document shredders |
| ☐ Secure destruction processes in place to industry standards utilising specialised 3rd party with disposal certificates produced |
| ☐ The secure transfer modes and encryption methods are regularly updated and kept state-of-the-art (e.g., according to the recommendations in the data protection manual issued by the BSI (Federal Office for Information Security)) |
| ☐ 3rd party secure off-site tape storage utilised |
| ☐ Secure communication session established via HTTPS and SFTP protocols across all applications / services |
| ☐ Encrypted certificates utilised for authentication between the web client and the web server across all websites |
| ☐ Other measures: _____ |
| 5. Input Control |
| Data importer shall take, among others, the following technical and organizational measures in order to ensure that it is subsequently possible to verify and establish whether and by whom personal data have been entered into data processing systems, altered or removed: |
| ☐ Access to electronic documents / applications is documented via auditable log files |
| ☐ Access to physical documents is documented via protocols |
| ☐ Protocolling input, modification and deletion of data by use of individual user names |
| ☐ Other measures: |
| 6. Control of Instructions |
| Data importer shall take, among others, the following technical and organizational measures in order to ensure that personal data which are processed on behalf of [Airwallex][Partner] can only be processed in compliance with [Airwallex][Partner]'s instructions: |
| ☐ Clear and binding internal policies contain formalized instructions for data processing procedures |

| |
|---|
| □ Unambiguous language in the underlying contracts |
| □ Careful selection of contractors, especially with regard to data security aspects |
| □ Internal monitoring of quality of service includes compliance with contractual arrangements |
| □ Regular audits by 3rd parties include compliance with contractual arrangements |
| □ Regular staff training to ensure compliance with contractual arrangements and maintain awareness regarding data protection requirements |
| □ Secure destruction processes in place to industry standards utilising specialised 3rd party with disposal certificates produced |
| □ Periodic risk assessments focus on how insider access is controlled and monitored |
| □ Data importer's corporate network is separated from its customer services network by means of complex segregation devices |
| □ Other measures: _____ |
| 7. Availability Control |
| Data importer shall take, among others, the following technical and organizational measures in order to protect the data from accidental destruction or loss: |
| □ Appliances for the monitoring of temperature and humidity |
| □ Fire / smoke detectors and fire extinguishers in the areas where data is stored / processed |
| □ State of the art firewall |
| □ Use of state-of-the-art anti-virus software that includes e-mail filtering and malware detection |
| □ Data recovery measures and emergency plan in place and regularly tested |
| □ Implementation of state-of-the-art backup methods such as: tape backup, data mirroring, and so on. Physical separation of the backup data. Data stored in the archive is saved using redundant systems. |
| □ Uses a combination of full, differential, and cumulative backups to ensure data integrity and timely restoration |
| □ Backup tapes are securely stored both on-site and off-site to provide protection against disaster and efficient data recovery |
| □ To ensure an uninterrupted supply of power to the system, redundant power supply units are built into the systems wherever possible. |
| □ Data is stored redundantly on multiple devices |
| □ Integrity of stored data regularly verified using checksums |
| □ Automated processes move data traffic away from affected area to uncompromised area in case of failure |
| □ Preventative maintenance is performed to ensure continued operability of equipment |
| □ Other measures: ____ |
| 8. Separation and Purpose Control |
| Data importer shall take, among others, the following technical and organizational measures in order to ensure that data collected for different purposes are processed separately: |
| □ Documents that are stored physically are stored separately for each customer and the respective containers are clearly labelled |
| □ Implementation of an authorization concept |
| □ Logical separation of electronically stored customer data (on the software side). Each client has its own designated database for storing information, to ensure that each client's data is isolated from any other client's data |
| □ Strong isolation between guest virtual machines is maintained. Customers are prevented from accessing areas not assigned to them by filtering through the virtualization software. |
| □ A unique encryption key is created per customer |
| □ Other measures: _____ |

## SCHEDULE 3

## APPROVED SUB-CONTRACTORS

As at the Effective Date, Data Discloser has given its approval for Data Recipient to engage the subcontractors set forth below for the purposes of the Project.

| **Name of Approved Sub-contractor** | **Role and Locations for which approval is granted** |
|---|---|
| [ ● ] | [ ● ] |
| [ ● ] | [ ● ] |