DATA PROCESSING ADDENDUM (V 1.3)

This Data Processing Addendum ("**Addendum**") supplements the agreement Surecomp Business Solutions Ltd. ("**Surecomp**" or "**Processor**") obtains with Customer ("**Client**" or "**Controller**") insofar as the agreement entered between Surecomp and Customer ("**Agreement**") includes the Processing of Personal Data (as defined below).

This Addendum shall apply only to the extent Surecomp Processes Personal Data subject to the GDPR.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended, and including, this Addendum.

1.   Definitions

1.1   In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1   "**Applicable Laws**" means the European Union law or any laws of a member state of the European Union in respect of which Surecomp or Client is subject to;

1.1.2   "**Client Personal Data**" means any Personal Data which may be Processed by Processor or a Sub-processor on behalf of Client, pursuant to or in connection with the Agreement; For purposes of clarity, the parties agree that Client Personal Data does not include data that is anonymized or de-identified in a manner that prevents the tracking or identification of any specific individual.

1.1.3   "**Data Protection Legislation**" means GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as amended from time to time or any regulation replacing the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

1.1.4   "**EU**" means the European Union;

1.1.5   "**EEA**" means the European Economic Area. The GDPR applies to the European Economic Area (EEA), which includes all EU countries as well as Iceland, Liechtenstein and Norway;

1.1.6   "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.7   "**EU SCC**" means the applicable model of the standard clauses for the transfer of Personal Data pursuant to the European Commission Implementing Decision (EU) 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 available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

1.1.8   "**Services**" means the services as defined in the Agreement;

1.1.9   "**Sensitive Data**" means Client Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Legislation, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) financial, credit, genetic, biometric or health information;(d) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences; and/or (c) account passwords in unleashed form.

1.1.10   "**Sub-processor**" means any person (excluding an employee of Surecomp) appointed by or on behalf of Surecomp to Process Client Personal Data in connection with the Agreement;

1.1.11   "**Supervisory Authority**" means (a) an independent public authority which is established by a member state of the European Union pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Legislation; and

1.1.12   "**Term**" means the term of the Agreement, as defined therein.

1.1.13   "**UK SCC**" means the EU Commission Standard Contractual Clauses or the International Data Transfer Agreement as issued by the UK Commissioner under S119A(1) of the Data Protection Act 2018, including any amended, extended, re-enacted or consolidated version in force from time to time, found at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf

1.2   The terms "**Controller**", "**Processor**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", and "**Processing**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Client Personal Data

2.1   The parties acknowledge that Client is the Controller and shall comply with the obligations of a Controller under the GDPR and that Surecomp is acting in the capacity of a Processor. In some circumstances, Client may additionally or alternatively be a Processor, in which case Client appoints Surecomp as an authorised Sub-processor, which shall not change the obligations of the parties under this Addendum as Surecomp will remain a Processor in any such event. Client will comply with all obligations applicable to a Controller pursuant to the Data Protection Legislation.

2.2   Surecomp shall Process Client Personal Data on the documented instructions of Client, unless otherwise required by an Applicable Law to which Surecomp is subject. In which case, Surecomp shall notify Client if, in its opinion, any instruction infringes the GDPR or other Applicable Law, unless that law prohibits such notification. Such notification will not constitute a general obligation on the part of Surecomp to monitor or interpret the laws applicable to Client, and such notification will not constitute legal advice to Client.

2.3   Client warrants that it has all the necessary rights to provide the Personal Data to Surecomp for the Processing to be performed in relation to the Services, and that one or more lawful bases set forth in the Data Protection Legislation support the lawfulness of the Processing. To the extent required by the Data Protection Legislation, Client is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another legal bases set forth in the Data Protection Legislation supports the lawfulness of the Processing, that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consent is maintained. Should such consent be revoked by a Data Subject, Client is responsible for communicating the fact of such revocation to Surecomp, and Surecomp will act pursuant to Client's instructions as seems appropriate.

2.4   **Annex 1** to this Addendum sets out certain information as required by Article 28(3) of the GDPR according to, Personal Data may be processed by Surecomp. Client warrants it is an accurate reflection of the Processing activities pursuant to this Addendum and the Agreement. The nature of the Processing operations will depend on the scope of the Services and the nature of the Personal Data that Client provides in its sole discretion, in a manner by which Surecomp finds appropriate to provide the required Services.

2.5   **Sensitive Data.** The Parties agree that the Services are not intended for the processing of Sensitive Data, and that if Client wishes to use the Services to process Sensitive Data, it must first obtain Surecomp's explicit prior written consent and enter into any additional agreements as required by Surecomp.

3. Confidentiality

Without prejudice to any existing contractual arrangements between the parties, Surecomp shall ensure that any person that it authorises to Process the Personal Data on its behalf, shall be subject to a duty of confidentiality that shall survive the termination of their employment and/or contractual relationship.

4. Security

4.1   Taken into account the measures required by Article 32 of the GDPR, and the state of the art, the costs of implementation and nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural person, Surecomp shall implement appropriate technical and organizational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk.

Such measures may be updated by Surecomp from time to time, provided that such updates shall not materially decrease the protection of Personal Data for Data Subjects. **Annex 2** attached to this Addendum demonstrates the security measures implemented by Surecomp.

4.2   Client acknowledges that the security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Client will therefore evaluate the measures implemented in accordance with section 4 on an on-going basis in order to maintain compliance with the requirements set forth in this section. The parties will negotiate in good faith, the cost, if any, to implement changes required by specific updated security requirements set forth in Data Protection Legislation or by data protection authorities of competent jurisdiction.

5.   Sub-processing

5.1   Client authorises Surecomp to appoint (and permit each Sub-processor to appoint) Sub-processors in accordance with **Annex 3** to this Addendum and any restrictions in the Agreement.

5.2   Surecomp shall notify Client of any intended changes concerning the addition or replacement of any of the Sub-Processors that will Process any Client Personal Data ("**New Sub-Processor**"). If, within 14 calendar days of receipt of that notice, Client notifies Surecomp in writing of any objections made on reasonable grounds, to the proposed appointment of a New Sub-Processor, the parties will endeavour to agree (acting reasonably), without undue delay, the commercially reasonable steps to be taken to ensure that the new Sub-processor is compliant with Article 28(4) of the GDPR.

5.3   In the absence of a resolution, Surecomp will make commercially reasonable efforts to provide Client with the same level of Service described in the Agreement, without using the objected Sub-Processor to Process Client Personal Data.

5.4   Where the Client reasonably argues that the risks involved with the sub-processing activities are still unacceptable, in the context of Article 28(4) and in relation to the appropriate steps, within the requisite time frame, the parties shall promptly seek to resolve the issues. Where the parties are unable to resolve the issues within such time frame, Client's sole remedy will be to terminate the Agreement.

5.5   With respect to each Sub-processors, Surecomp shall ensure that the Sub-processor is bound by data protection obligations compatible with those of the Data Processor under this Addendum.

6.   Data Subject Rights

6.1   Client shall comply with requests received from Data Subjects to exercise their rights pursuant to Chapter III of the GDPR or Data Protection Legislation.

6.2   Surecomp shall not directly reply to a Data Subjects request to exercise their rights pursuant to Chapter III of the GDPR. If such requests from Data Subjects to exercise their rights is received directly by Surecomp, Surecomp will forward Client the request or correspondence. When Client is unable to perform according to section 6.1, and therefore requires Surecomp's assistance, while taking into account the nature of the Processing, Surecomp shall assist Client, upon Client's request and at the Client's cost, by using appropriate technical and organisational measures, insofar as this is possible to comply with requests to exercise data protection rights, under the Data Protection Legislation.

7.   Personal Data Breach

7.1   When Surecomp becomes aware of an incident that has a material impact on the Processing of Personal Data that is the subject to the Agreement, it shall notify Client without any undue delay, and in no event longer than 48 hours after Surecomp discovers the security incident. Surecomp shall cooperate with Client and follow Client's instructions with regard to such incidents, to enable Client to perform an investigation into the incident, formulate a correct response and take suitable further steps in respect to the incident.

7.2   Except as required by law, Surecomp will not take action to notify Data Subjects of any security incident. Notwithstanding, where the incident is reasonably likely to require a data breach notification by Client under the Data Protection Legislation, Surecomp will assist Client, at the Client's cost with the notification process.

7.3   On the basis of such notification, where applicable Client shall notify the Personal Data Breach to the competent Supervisory Authority in accordance with Article 33 of the GDPR and to the extent required, shall communicate

the required information regarding the Personal Data Breach to the Data Subject in accordance with Article 34 of the GDPR.

7.4   Surecomp shall, at Client's cost, cooperate with Client and take the reasonable commercial steps which shall reasonably be instructed by Client, to assist in the investigation and mitigation of every occurring Personal Data Breach.

8.   Deletion or Return of Client Personal Data

8.1   Subject to section 8.2, Client may in its discretion by written notice to Surecomp within 30 calendar days of the cessation date, require Surecomp to (a) return a complete copy of all Client Personal Data which is in Surecomp's possession and/or control, to the Client; and (b) delete all other copies of Client's Personal Data Processed by Processor and which are in Surecomp's possession and/or control. Surecomp shall comply with any such written request within 60 calendar days of the cessation date.

8.2   The above requirement shall not apply to the extent Processor is required by Applicable Laws, to retain some and/or all of Client Personal Data, or to Client Personal Data which Surecomp has archived on back-up systems (e.g., in the form of audit logs), which Surecomp shall securely isolate and protect from any further Processing, except to the extent required by the Applicable Law.

9.   Audit Rights

9.1   Subject to section 9.2 and 9.3, Surecomp shall make available to Client upon a reasonable request and at Client's cost, information which is reasonably necessary to demonstrate compliance with Article 28(3) of the GDPR.

9.2   Where applicable, if Client is not otherwise satisfied by its audit rights pursuant to the Agreement, Surecomp shall, at the Client's costs, allow for audits, including inspections, by an auditor mandated by Client (subject to section 9.3 where auditor shall be subject to written confidentiality obligations in relation to such information) in relation to the Processing of the Client's Personal Data by the Processor, provided that:

   9.2.1   Client shall give Surecomp a reasonable notice of any audit or inspection to be conducted and shall schedule such audit with Surecomp; and

   9.2.2   Client shall take reasonable steps to ensure (and shall procure that each of its mandated auditors) to minimize disruption to the Processor's business, in the course of such audit or inspection, while such audits or inspections shall be conducted during normal working hours.

   9.2.3   The auditor shall have no access to non-Client information.

   9.2.4   no audit shall include access to Surecomp's network and/ or networks that contain Surecomp's other clients' data;

   9.2.5   Client will receive only the auditor's report, without any Surecomp 'raw data' materials, will keep the audit results in strict confidentiality and will use them solely for the specific purposes of the audit under this section;

   9.2.6   At Surecomp'a request, Client will provide it with a copy of the auditor's report;

   9.2.7   As soon as the purpose of the audit is completed, Client will permanently dispose of the audit report.

9.3   Surecomp may object to an auditor mandated by Client if the auditor is, in Surecomp's opinion, not suitably qualified or independent, a competitor of Surecomp, or otherwise manifestly unsuitable. In the event of such an objection, Client shall appoint another auditor or conduct the audit itself.

9.4   Such audit or inspection may be conducted up to one time per each 12 months' term.

10.   Transfers

10.1   Personal Data may be transferred from EU Member States, the three EEA member countries, Switzerland and the United Kingdom ("UK") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the EU, the Member States or the European Commission, or Switzerland or the UK as relevant ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.

10.2   Information may be transferred to third party companies and individuals to facilitate Surecomp's Services, who are located in a country which have not been subject to a relevant Adequacy Decision ("**Cross Border Transfer**"). To the extent that Cross Border Transfer occurs by Surecomp or its Sub-processors with respect to the transfer of Client Personal Data, the following shall apply: (i) the terms set forth in Article A of the Cross-Border Transfer Schedule (EEA Cross Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in Article B of the Cross-Border Transfer Schedule (UK Cross Border Transfers) shall apply to any such UK Transfer; (iii) the terms set forth in Article C of the Cross-Border Transfer Schedule (Switzerland Cross Border Transfers) shall apply to any such Swiss Transfer.

10.3   In addition, with respect to each such data transfer, Surecomp shall implement appropriate technical and organizational measures to ensure a level of security, appropriate to the risk, while taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing as well as the likelihood of a risk to the rights and freedoms of natural persons.

10.4   To the extent that Surecomp or Client are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently modified, revoked, or held in a court of a competent jurisdiction to be invalid, Surecomp or Client agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

11.   General Terms

Liability and Indemnity

11.1   Client shall indemnify Surecomp and will hold Surecomp harmless against all claims, losses, damages and expenses incurred by Surecomp arising out of a breach of this Addendum and/or the Data Protection Legislation by Client, or arising from any claim which Surecomp receives from a Data Subject and/or a Supervisory Authority, which is pursuant to a Data Subject claim.

11.2   Furthermore, Client shall indemnify Surecomp for any expenses incurred by it when cooperating or assisting Client to comply with a request submitted by a Data Subject pursuant to Section 6.2 above.

11.3   In no event shall Surecomp or anyone on its behalf (or its affiliates) be liable for any indirect, consequential, incidental, special or punitive damages of any kind incurred. Notwithstanding anything to the contrary herein, under no circumstances will Surecomp's (or any of its affiliates') total and aggregate liability to Client (and all its affiliates) arising out of or related to this DPA shall exceed the limitation of liability cap set forth in the Agreement to which this DPA is attached too. For the avoidance of doubt, Surecomp's and its affiliates' total liability for all claims from the Client arising out of or related to the Agreement and the DPA shall apply in the aggregate for all claims under both the Agreement and the DPA and not separately.

Order of Precedence

11.4   With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement, the provisions of this Addendum shall prevail.

Changes in Data Protection Legislation

11.5   If any variation is required to this Addendum as a result of a change in Data Protection Legislation, then either party may provide written notice to the other party of that change of law. The parties shall discuss the change in Data Protection Legislation and negotiate in good faith with a view to agreeing on any necessary variations to this Addendum to address such changes, including any resulting charges.

Governing Law and Jurisdiction

11.6   This Addendum is governed by the laws of England and Wales. Any disputes arising from or in connection with this Addendum, shall be brought exclusively before the competent court of London, UK.

Severance

11.7   Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Corporate Use

ANNEX 1: DETAILS OF PROCESSING OF CLINET PERSONAL DATA

This Annex 1 includes certain details of the Processing of the Client's Personal Data as required by Article 28(3) GDPR.

Subject Matter and Duration of the Processing of Client Personal Data

The subject matter and duration of the Processing of Client Personal Data are set out in the Agreement and this Addendum.

The Nature and Purpose of the Processing of the Designated Controller's Personal Data

Surecomp provides Client with trade finance solutions in the course of which Surecomp may receive access and Process Client Personal Data.

Special Categories of Personal Data to be Processed [i.e. g racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation]

No special category data is collected.

The Categories of Data Subject to whom the Personal Data Relates

Client's Users authorized by Client to use the Services

The Obligations and Rights of Surecomp

The obligations and rights of the parties are set out in the Agreement and this Addendum.

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Surecomp utilizes Amazon Web Services ("**Cloud Provider**") and relies to a great extent on the technical security measures adopted by Cloud Provider. In addition to the security measures adopted by Cloud Provider, and to the extent data processing activities occur outside the Cloud provider system, Surecomp has implemented the following technical and organizational measures to ensure the security of Client Personal Data:

1. Unauthorised persons are prevented from gaining physical access to Surecomp's premises and the rooms where data processing systems are located.

2. Employees are only allowed access to tasks assigned to them.

3. Surecomp uses video surveillance and alarm devices with reference to access areas.

4. Surecomp Personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times.

5. Surecomp ensures that all computers processing personal data (including computers with remote access) are password protected, both after booting up and when left, even for a short period.

6. Surecomp assigns individual user passwords for authentication.

7. Surecomp only grants system access to its authorised personnel and strictly limit their access to applications required for those personnel to fulfil their specific responsibilities.

8. Surecomp has implemented a password policy that prohibits the sharing of passwords, outlines procedures to follow after disclosure of a password, and requires that passwords be changed regularly.

9. Surecomp ensures that passwords are always stored in encrypted form.

10. Surecomp adopted procedures to deactivate user accounts when an employee, agent, or administrator leaves Consensus or moves to another responsibility within the company.

11. Surecomp prevents the installation and use of unauthorized hardware and software on its premise.

12. Surecomp has established rules for the safe and permanent destruction of data that are no longer required.

13. Except as necessary for the provision of the Services, Client Personal Data cannot be read, copied, modified or removed without authorization during transfer or storage.

14. Surecomp encrypts data during any transmission.

15. Surecomp is able to retrospectively examine and establish whether and by whom Client Personal Data has been entered into data processing systems, modified or removed.

16. Surecomp logs administrator and user activities, and regularly trains its staff on data privacy and data security.

17. Surecomp process the personal data received from different clients so that in each step of the processing and each client can be identified and data is always physically or logically separated.

18. Surecomp creates back-up copies stored in protected environments.

19. Surecomp performs regular restore tests from its backups.

20. Surecomp has created business recovery strategies.

21. Surecomp does not use personal data for any purpose other than what have been contracted to perform.

22. Surecomp does not remove Client Personal Data from its business computers or premises for any reason (unless client had specifically authorised such removal for business purposes).

23. Whenever a user leaves his or her desk unattended during the day and prior to leaving the office at the end of the day, he or she is required to place any documents containing Client Personal Data in a secure environment such as a locked desk drawer, filing cabinet, or other secured storage space.

24. Surecomp ensures that each computer system runs a current anti-virus solution.

25. Surecomp has designated a responsible person to perform the functions of a data protection officer.

26. Surecomp has obtained the written commitment of its employees to maintain confidentiality and to comply with its requirements under the Addendum and the GDPR.

Corporate Use

Surecomp

ANNEX 3 – List of Sub-processors

Subprocessor	Services provided to Surecomp	Location of the Processing (country)
Amazon	Hosting	USA
Surecomp Development Ltd.	Support	Israel
Surecomp Asia Pacific Pte. Ltd.	Support	Singapore
Surecomp Inc. Latin America Ltda.	Support	Chile
Surecomp DOS GmbH & Co.KG	Support	Germany
Enigio Time AB	Third Party Application	Sweden
Signicat AB	Third Party Application	Sweden

Last Updated: March 2023

Corporate Use

Cross-Border Transfer Schedule

Article A - EEA Cross Border Transfers

1. In case the Processing of Client Personal Data by Surecomp's requires an EEA Cross Border Transfer of Client's Personal Data, the applicable Module 2 (Controller – Processor) or Module 3 (Processor – SubProcessor) of the EU SCC shall apply and incorporated to this DPA, including the following terms:

   1.1. In Clause 7, the optional docking clause will apply;

   1.2. In Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 5 of this DPA;

   1.3. In Clause 11, the optional language will not apply;

   1.4. In Clause 17, Option 2 will apply, and the Parties agree that the EU SCC shall be governed by the laws of Ireland;

   1.5. In Clause 18(b), disputes shall be resolved before the courts of Ireland;

   1.6. Annex I of the EU SCCs shall be deemed completed with the information set out in ANNEX 1 to this DPA;

   1.7. Annex II of the EU SCCs shall be deemed completed with the information set out in ANNEX 2 to this DPA; and

   1.8. Annex III of the EU SCCs shall be deemed completed with the information set out in ANNEX 3 to this DPA.

Article B – UK Cross Border Transfer
Table 1:

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Client Main address (if a company registered address): As set forth in the Agreement Official registration number: As set forth in the Agreement	Surecomp Main address (if a company registered address): As set forth in the Agreement Official registration number: As set forth in the Agreement
Key Contact	As set forth in the Agreement	As set forth in the Agreement
Importer Data Subject Contact		As set forth in the Agreement
Signatures confirming each Party agrees to be bound by this IDTA	By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.	By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses: as set forth in Article A of this Cross-Border Transfer Schedule.
Table 3: Transferred Data. As set forth in Annex 1.
Table 4: Security Requirements. As set forth in Annex 2.

1. Entering into this Article B: Each Party agrees to be bound by the terms and conditions set out in this Article B, in exchange for the other Party also agreeing to be bound by this Article B and the UK SCC and its UK Addendum.

2. Although Annex 1 and Clause 4 of the UK SCC requires signature by the Parties, for the purpose of making UK Transfers, the Parties may enter into this Article B in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Article B.

3. Entering into this Article B will have the same effect as signing the EU SCC and any part of the EU SCC.

4. **Interpretation of this Article B**. Where this Article B uses terms that are defined in the EU SCC, those terms shall have the same meaning as in the EU SCC. In addition, the following terms have the following meanings:

Appendix Information	The information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in Annex 1, Annex 2 and Annex 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when the Parties are making a UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
ICO	The Information Commissioner.
Article B	This Article B which is made up of this Article B incorporating the Addendum EU SCCs.
UK Addendum	An addendum to the Standard Contractual Clauses published by the ICO and approved by the UK Parliament.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Transfer	A transfer which is covered by Chapter V of the UK GDPR.

5. This Article B must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Article B, UK Data Protection Laws applies.

7. 7. If the meaning of this Article B is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this DPA has been entered into.

9. If the Parties wish to change the format of the information included in Tables 1, 2 or 3 of this Article B, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

Article C – Switzerland Cross Border Transfer

The Parties agree that the Standard Contractual Clauses as detailed in Article A of this Cross-border Transfer Schedule, shall be adjusted as set out below where the Federal Act on Data Protection of 19 June 1992 (the "FADP", and as revised as of 25 September 2020, the "Revised FADP") applies to Switzerland Transfers:

1. References to the Standard Contractual Clauses means the Standard Contractual Clauses as amended by this Article C;

2. The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory Authority for Switzerland Transfers exclusively subject to the FADP;

3. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Switzerland Transfers.

4. References to Regulation (EU) 2018/1725 are removed.

5. Switzerland Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Table 1 of Article B of this Cross-border Schedule;

6. References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;

7. Where Switzerland Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP;

8. Where Switzerland Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FDPA insofar as the Switzerland Transfers are subject to the FADP;

9. The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the Revised FADP.

Corporate Use