CONTROLLER-TO-CONTROLLER DATA PROTECTION ADDENDUM

This Data Protection Addendum (including its Exhibits) ("**Addendum**") forms part of and is subject to the terms and conditions of the [insert name of agreement] (the "**Agreement**") by and between [insert Moloco legal entity] ("**Moloco**") and [insert Service Provider legal entity] ("**Service Provider**").

1. Subject Matter and Duration.

1.1. Subject Matter. This Addendum reflects the parties' commitment to abide by Data Protection Laws concerning the Processing of Moloco Personal Data in connection with the execution of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

1.2. Duration. This Addendum will become legally binding upon the effective date of the Agreement or upon the date that the parties sign this Addendum if it is completed after the effective date of the Agreement. Service Provider's obligations and Moloco's rights under this Addendum will continue in effect so long as Service Provider Processes Moloco Personal Data.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

2.1. "**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Moloco Personal Data are subject. "Data Protection Laws" may include, but are not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).

2.2. "**Moloco Personal Data**" means Personal Data Processed by Service Provider in connection with the Agreement.

2.3. "**Permitted Purpose(s)**" means [Moloco to insert. E.g., "Service Provider's Processing of Moloco Personal Data as required to provide the contracted services to Moloco under the Agreement."]

2.4. "**Personal Data**" has the meaning assigned to the terms "personal data" or "personal information" under applicable Data Protection Laws, and will, at a minimum, mean any information relating to an identified or identifiable natural person.

2.5. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.6. "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Moloco Personal Data.

2.7. "**Subprocessor(s)**" means Service Provider's vendors, service providers, and other third parties that Process Moloco Personal Data.

3. Processing Terms for Moloco Personal Data.

3.1. Service Provider's Role Under Data Protection Laws. Service Provider is a separate "Business" and/or independent "Controller" (as such terms are defined by Data Protection Laws) of Moloco Personal Data. Under no circumstances shall the parties be considered joint "Controllers" under Data Protection Laws.

3.2. Use of Moloco Personal Data. Service Provider shall Process Moloco Personal Data solely for the Permitted Purpose, and solely to the extent necessary to carry out the Permitted Purpose, in each case, in accordance with the Agreement, this Addendum, and Data Protection Laws. Service Provider and its Subprocessors shall not Process Moloco Personal Data to develop, commercialize, license or sell any product, service or technology that could, directly or indirectly, compete with Moloco's products and services.

3.3. Transparency. Service Provider shall maintain a publicly available privacy notice that clearly and accurately describes its practices with respect to its collection, use, and disclosure of Moloco Personal Data.

Commented [FW1]: Cortlandt: Feel free to adjust the definition of Moloco Personal Data and the Permitted Purposes as appropriate to reflect expectations for the agreement

3.4. Service Provider and Subprocessor Compliance. Service Provider shall (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Moloco Personal Data that imposes on such Subprocessors use restrictions and data protection and information security requirements for Moloco Personal Data that are at least as protective as the obligations in this Addendum; and (ii) remain fully liable to Moloco for Service Provider's Subprocessors' failure to perform their obligations with respect to the Processing of Moloco Personal Data.

3.5. Confidentiality. Any person authorized to Process Moloco Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

3.6. Personal Data Inquiries and Requests. Service Provider shall, to the extent legally permitted, promptly notify Moloco if it receives a request from a data subject to exercise an individual right under Data Protection Laws or otherwise, including rights for access to, or correction, amendment, blocking, restriction, or deletion of that data subject's Moloco Personal Data, only if such request may impact Moloco's Processing of Moloco Personal Data. Service Provider shall independently, timely, and fully address any data subject's request to exercise rights under Data Protection Law or otherwise.

3.7. Data Protection Impact Assessment and Prior Consultation. Service Provider agrees to provide reasonable assistance to Moloco where, in Moloco's judgement, the type of Processing performed in connection with the Agreement requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

3.8. Demonstrable Compliance. Service Provider agrees to provide information reasonably necessary to demonstrate compliance with this Addendum upon Moloco's reasonable request.

4. Information Security Program.

4.1. Security Measures. Service Provider shall implement and maintain reasonable administrative, technical, and physical safeguards that protect Moloco Personal Data (the "**Information Security Program**"). At a minimum, such safeguards shall include:

4.1.1. Pseudonymisation of Moloco Personal Data where appropriate, and encryption of Moloco Personal Data in transit and at rest;

4.1.2. The ability to ensure the ongoing confidentiality, integrity, availability of Service Provider's Processing and Moloco Personal Data;

4.1.3. The ability to restore the availability and access to Moloco Personal Data in the event of a physical or technical incident;

4.1.4. A process for regularly testing, assessing and evaluating the effectiveness of the Service Provider's Information Security Program to ensure the security of its Processing and Moloco Personal Data.

5. Security Incidents.

5.1. Security Incident Procedure. Service Provider will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Moloco Personal Data in a timely manner.

5.2. Notice. Service Provider agrees to provide written notice without undue delay (but in no event longer than twenty-four (24) hours) to Moloco's Designated POC if it knows or reasonably suspects that a Security Incident has taken place. Such notice will include all reasonably available details relevant to the Security Incident. Moloco may request additional information related to the Security Incident following Service Provider's notice and Service Provider shall provide such information within a reasonable period of time.

5.3. Remediation. Service Provider shall: (i) investigate, remediate and take any other action Moloco deems necessary regarding the Security Incident; (ii) provide full cooperation and assistance to Moloco in connection with Moloco's remediation and mitigation efforts and any dispute, inquiry, investigation, claim, or order concerning the Security Incident; and (iii) provide Moloco with assurance satisfactory to Moloco that such Security Incident will not recur. Service Provider shall be solely responsible to notify government authorities and data subjects of any Security Incident experienced by Service Provider provided that, except for counsel, relevant advisors and as otherwise required by applicable law, Service Provider will not communicate with any third party, including, but not limited to any government authority, the media, and affected data subjects regarding any Security Incident in a manner that directly or indirectly references Moloco without the express written

consent of Moloco. Notwithstanding the foregoing, if a Security Incident affects both parties, the parties agree to coordinate with respect to any communications or notifications that are sent to government authorities and/or data subjects regarding such Security Incident. Service Provider will be fully liable for all costs and expenses incurred by Service Provider and/or Moloco in connection with the Security Incident.

6. Cross-Border Transfers of Moloco Personal Data.

6.1. Cross-Border Transfers of Moloco Personal Data. Moloco authorizes Service Provider to transfer Moloco Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States, provided that such transfer complies with Data Protection Laws.

6.2. If Moloco Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by or on behalf of Moloco to Service Provider in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by Module One's obligations in the Annex to the 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 ("**Standard Contractual Clauses**") as supplemented by **Exhibit A** attached hereto, the terms of which are incorporated herein by reference. Each party's signature to the [Addendum/Agreement] shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

7. Audits.

7.1. Moloco Audit. Moloco (or its appointed representative) may carry out an audit, assessment, and/or inspection of Service Provider's premises, architecture, systems, policies, procedures, and records relevant to the Processing of Moloco Personal Data. Any audit, assessment, or inspection must be: (i) conducted during Service Provider's regular business hours; (ii) with reasonable advance notice to Service Provider; (iii) carried out in a manner that prevents unnecessary disruption to Service Provider's operations; and (iv) subject to reasonable confidentiality procedures.

7.2. Third-Party Audit. Further, Service Provider may, with Moloco's consent, arrange for a qualified and independent auditor or assessor to conduct, at least annually and at Service Provider's expense, an audit or assessment of Service Provider's policies and technical and organizational measures in support of the obligations under Data Protection Laws and this Addendum using an appropriate and accepted control standard or framework and audit/assessment procedure for such audits or assessments, as applicable. Service Provider shall provide a report of the audit or assessment to Moloco upon request.

7.3. Remediation. Following an audit, assessment, or inspection, Service Provider shall make any necessary changes to ensure compliance with its obligations under this Addendum at its own expense and without unreasonable delay and shall notify Moloco when such changes are complete.

8. Moloco Personal Data Storage and Deletion.

8.1. Data Storage. Service Provider will not store or retain any Moloco Personal Data except as necessary to carry out the Permitted Purposes.

8.2. Data Deletion. Service Provider will abide by the following with respect to deletion of Moloco Personal Data:

8.2.1. Within thirty (30) calendar days of the Agreement's expiration or termination, or sooner if requested by Moloco, Service Provider will securely destroy (per subsection (8.2.3) below) all copies of Moloco Personal Data (including automatically created archival copies).

8.2.2. Upon Moloco's request, Service Provider will promptly return to Moloco a copy of all Moloco Personal Data within thirty (30) days and, following such return, will also delete all Moloco Personal Data as set forth above.

8.2.3. Moloco Personal Data shall be disposed of in a method that prevents any recovery of the data in accordance with industry best practices for shredding of physical documents and wiping of electronic media (e.g., NIST SP 800-88).

8.2.4. Upon Moloco's request, Service Provider will provide a "Certificate of Deletion" certifying that Service Provider has deleted all Moloco Personal Data. Service Provider will provide the "Certificate of Deletion" within thirty (30) days of Moloco's request.

9. Indemnification.

9.1. Indemnity. Service Provider shall indemnify, defend, and hold harmless Moloco and its officers, directors, employees and agents from and against any claims, disputes, demands, liabilities, damages, losses, fines, and costs and expenses, including, without limitation, reasonable attorneys' fees arising out of or relating to: (i) a Security Incident; or (ii) Service Provider's breach of this Addendum. Service Provider's obligations under this Addendum shall not be subject to any limitation or exclusion of liability provision in the Agreement. This Section 9 shall survive termination of the Agreement.

10. Miscellaneous.

10.1. Disputes and Claims. In the event of an inquiry, dispute, or claim brought by a data subject or a government authority concerning Service Provider's Processing of Moloco Personal Data, Service Provider will inform Moloco about any such inquiry, dispute, or claim, and will cooperate with Moloco with a view to resolving them within a reasonable time.

10.2. Remediation of Processing. Upon notice from Moloco, Service Provider shall immediately remediate any Processing of Moloco Personal Data that Moloco reasonably believes violates an applicable privacy policy, notice, or similar document or impacts Moloco's Processing of such Moloco Personal Data, or Moloco's compliance with Data Protection Laws.

11. Contact Information.

11.1. Moloco and Service Provider agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- **Moloco Designated POC:** _____
- **Service Provider Designated POC:** _____

IN WITNESS WHEREOF, the duly authorized representatives of the parties have executed this Addendum effective as of the last date signed below.

[insert Moloco legal entity]	**[insert Service Provider legal entity]**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A TO THE DATA PROTECTION ADDENDUM

This Exhibit A forms part of the Addendum and supplements the Standard Contractual Clauses. Capitalized terms not defined in this Exhibit A have the meaning set forth in the Addendum.

The parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. **Supplemental Terms.** The parties agree that: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection."; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III)."; (iii) the optional text in Clause 7 is deleted; (iv) the optional text in Clause 11 is deleted; and (v) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. **Annex I.** Annex I to the Standard Contractual Clauses shall read as follows:

A. List of Parties

Data Exporter: Moloco.
Address: As set forth in the Notices section of the Agreement.
Contact person's name, position, and contact details: Moloco Designated POC.
Activities relevant to the data transferred under these Clauses: As set forth in the Addendum.
Role: Controller.

Data Importer: Service Provider.
Address: As set forth in the Notices section of the Agreement.
Contact person's name, position, and contact details: Service Provider Designated POC.
Activities relevant to the data transferred under these Clauses: As set forth in the Addendum.
Role: Controller.

B. Description of the Transfer:

Categories of data subjects whose personal data is transferred: The categories of data subjects whose personal data is transferred under the Clauses including, but not limited to, [insert examples].
Categories of personal data transferred: The categories of personal data that are transferred under the Clauses including, but not limited to, [insert examples].
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: **CHOOSE ONE:** [To the parties' knowledge, no sensitive data is transferred.] **OR** [Sensitive data that is transferred under the Clauses including, but not limited to, [insert examples].]
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with the standard functionality of the technology used by the parties, or as otherwise agreed upon by the parties.
Nature of the processing: As set forth in the Addendum.

Purpose(s) of the data transfer and further processing: As set forth in the Addendum.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data importer will retain personal data in accordance with the Addendum.

C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

D. Additional Data Transfer Impact Assessment Questions for Data Importer:

What countries will personal data that is transferred under the Clauses be stored in or accessed from? If this varies by region, please specify each country for each region.

[Service Provider to insert response. E.g., "United States."]

Will data importer process any personal data that is transferred to the United States under the Clauses about a non-United States person that could reasonably be considered "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)?

[Service Provider to insert response. E.g., "Not to data importer's knowledge."]

Is data importer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where personal data is stored or accessed from that would interfere with data importer fulfilling its obligations under the Clauses? For example, FISA Section 702. If yes, please list these laws:

[Service Provider to insert response. E.g., "As of the effective date of the Addendum, no court has found data importer to be eligible to receive process issued under the laws contemplated by this question, including FISA Section 702, and no such court action is pending."]

Has data importer ever received a request from public authorities for information pursuant to the laws contemplated by the question above? If yes, please explain:

[Service Provider to insert response. E.g., "No."]

Has data importer ever received a request from public authorities for personal data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain:

[Service Provider to insert response. E.g., "No."]

E. Data Transfer Impact Assessment Outcome: Taking into account the information and obligations set forth in the Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the personal data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the Clauses to a country that has not been found to provide an adequate level of protection under applicable data protection laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable data protection laws.

3. **Annex II.** Annex II of the Standard Contractual Clauses shall read as follows:

Data importer shall implement and maintain appropriate technical and organisational measures that protect personal data in accordance with the Addendum.

4. **Annex III.** A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the Addendum. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the Addendum.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Clauses.

Table 4: The parties agree that Exporter may end the UK Addendum as set out in Section 19.