EXHIBIT A
TO THE
DROP SHIP SUPPLIER AGREEMENT

DATA PROCESSING ADDENDUM

This **DATA PROCESSING ADDENDUM** ("**DPA**") is by and between Legends and Supplier. This DPA is incorporated into and forms part of the Drop Ship Supplier Agreement ("**Agreement**") entered into by and between the Parties. In the event of any conflict between this DPA and the remainder of the Agreement, the terms of this DPA shall prevail. Each party may be referred to herein each as a "**Party**" or collectively as the "**Parties**."

I. DEFINITIONS

A. Capitalized terms used but not defined in this DPA will have the meaning set forth in the Agreement. The following capitalized terms used in this DPA will be defined as follows:

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time.

"**Covered Data**" means Personal Data that is: (a) provided by or on behalf of Legends to Processor in connection with the Services; or (b) obtained, developed, produced or otherwise Processed by Processor, or its agents or subcontractors, for purposes of providing the Services.

"**Data Subject**" means a natural person whose Personal Data is Processed.

"**Deidentified Data**" means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"**EEA**" means the European Economic Area including the European Union ("**EU**").

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 or, where applicable, the equivalent provision under Swiss data protection law.

"**Legends Affiliate**" means an affiliate of Legends.

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein.

"**Personal Data**" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Security Incident**" means an actual or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

"**Services**" means the processing and fulfilment of Orders and related services to be provided by Supplier under the Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"**Sub-processor**" means an entity appointed by Supplier to Process Covered Data on its behalf.

"UK" means the United Kingdom.

"**US Data Protection Laws**" means, to the extent applicable, federal and state laws relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States.

II. PROCESSING TERMS

A. Any Processing operation as described in clause IV (Details of Data Processing) and **<u>SCHEDULE 1</u>** to this DPA will be subject to this DPA.

B. Legends Affiliates will be beneficiaries under this DPA and be entitled to enforce all rights in relation to Covered Data provided by the respective Legends Affiliate. Legends will be the only point of contact for all communication between Legends Affiliates and Supplier.

III. ROLE OF THE PARTIES

A. The Parties acknowledge and agree that:

1. For the purposes of the GDPR, Supplier acts as "processor" (as defined in the GDPR) on behalf of Legends.

2. For the purposes of the US Data Protection Laws, Supplier will act as a "service provider" or "processor" (as defined in US Data Protection Laws), as applicable, in its performance of its obligations pursuant to this DPA.

IV. DETAILS OF DATA PROCESSING

A. The details of the Processing of Personal Data this DPA (such as subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in **<u>SCHEDULE 1</u>** to this DPA.

B. Supplier shall Process Covered Data solely on behalf of and under the instructions of Legends and in accordance with Applicable Data Protection Laws and any other applicable laws. This DPA will generally constitute instructions for the Processing of Covered Data. Legends may issue further written instructions in accordance with this DPA. Without limiting the foregoing, Supplier is prohibited from:

1. selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration;
2. sharing Covered Data with any third party for cross-context behavioral advertising;
3. retaining, using, or disclosing Covered Data for any purpose other than for the business purposes specified in this DPA or as otherwise permitted by Applicable Data Protection Laws;
4. retaining, using, or disclosing Covered Data outside of the direct business relationship between the Parties; and
5. except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that Supplier receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

C. Supplier will limit access to Covered Data to personnel who have a business need to have access to such Covered Data, and will ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA.

D. Supplier may (without prejudice to clause XI) Process Covered Data anywhere that Supplier or its Sub-processors maintain facilities, subject to clause V of this DPA.

E. Supplier will provide Legends with information to enable Legends to conduct and document any data protection assessments required under Applicable Data Protection Laws. In addition, Supplier will notify Legends promptly if Supplier determines that it can no longer meet its obligations under Applicable Data Protection Laws.

F. Legends will have the right to take reasonable and appropriate steps to ensure that Supplier uses Covered Data in a manner consistent with Legends's obligations under Applicable Data Protection Laws.

V. SUB-PROCESSORS

A. Legends grants Supplier the general authorization to engage Sub-processors, subject to clause V(B), as well as Supplier's current Sub-processors listed in **SCHEDULE 4** as of the Effective Date.

B. Supplier will (i) enter into a written agreement with each Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than Supplier's obligations under this DPA; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA.

C. Supplier will provide Legends with at least thirty (30) days' notice of any proposed changes to the Sub-processors it uses to Process Covered Data. Legends may object to Supplier's use of a new Sub-processor (including when exercising its right to object under clause 9(a) of the SCCs if applicable) by providing Supplier with written notice of the objection within thirty (30) days after Supplier has provided notice to Legends of such proposed change (an "**Objection**"). If Legends does not object to the engagement within the Objection period, consent regarding the engagement will be assumed. In the event Legends objects to Supplier's use of a new Sub-processor, Legends and Supplier will work together in good faith to find a mutually acceptable resolution to address such Objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Legends may direct Supplier to terminate the Processing activities relating to the Services affected by such change by providing written notice to the other Party. During any such Objection period, Supplier may suspend the affected portion of the Services.

VI. DATA SUBJECT RIGHTS REQUESTS

A. As between the Parties, Legends will have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Covered Data under Applicable Data Protection Laws (each, a "**Data Subject Request**").

B. Supplier will promptly forward to Legends without undue delay any Data Subject Request received by Supplier or any Sub-processor and may advise the individual to submit their request directly to Legends.

C. Supplier will provide Legends with reasonable assistance as necessary for Legends to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests, including if applicable, Legends's obligation to respond to requests for exercising the rights set out in Applicable Data Protection Laws.

VII. SECURITY AND AUDITS

A. Supplier will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure security of Covered Data, including, without limitation, protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage of or to it. When assessing the appropriate level of security, account will be taken in particular of the nature, scope, context and purpose of the Processing as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data.

B. Supplier will implement and maintain as a minimum standard the measures set out in **SCHEDULE 2**.

C. Legends will have the right to audit Supplier's compliance with this DPA. The Parties agree that all such audits will be conducted:

1. upon reasonable written notice to Supplier;

2. only once per year, or more frequently if any audit indicates that Supplier is in non-compliance with this DPA; and

3. only during Supplier's normal business hours.

D. To conduct such audits, Legends may engage a third-party auditor subject to such auditor complying with the requirements under clause VII(C) and provided that such auditor is suitably qualified and independent.

E. Legends will promptly notify Supplier of any non-compliance discovered during an audit.

F. Promptly after the Effective Date, and thereafter upon request, Supplier will provide to Legends documentation reasonably evidencing the implementation of the technical and organizational data security measures in accordance with industry standards. Supplier may, in its discretion, provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company.

G. If the scope of any audit to be conducted by Legends or a third-party auditor under clause VII(C) or clause VII(D) is addressed in the certifications provided by Supplier under clause VII(F) and produced by a qualified third-party auditor within twelve (12) months of Legends's audit request, and Supplier confirms there are no known material changes in the controls audited, Legends agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

H. Supplier will audit its Sub-processors on a regular basis and will, upon Legends's request, confirm their compliance with Applicable Data Protection Laws and the Sub-processors' contractual obligations.

I. In the event that Supplier fails to provide Legends with any of the documentation required under clause VII(F), Legends may, without prejudice to its rights under Section **Error! Reference source not found.** of the Agreement, cancel (in whole or in part) any unshipped Orders and suspend or terminate Supplier's account and status as Legends' authorized supplier of Goods until such time as Supplier remedies any non-compliance with clause VII(F), in each case on written notice to Supplier with immediate effect, and without liability, cost or charge to Legends.

VIII. SECURITY INCIDENTS

Supplier will notify Legends in writing without undue delay, and in any event within twenty-four (24) hours, after becoming aware of any Security Incident, and reasonably cooperate in any obligation of Legends under Applicable Data Protection Laws to make any notifications, such as to individuals or supervisory authorities. Supplier will take reasonable steps to contain, investigate, and mitigate any Security Incident, and will send Legends timely information about the Security Incident, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation. Supplier's notification of or response to a Security Incident under this clause VIII will not be construed as an acknowledgement by Supplier of any fault or liability with respect to the Security Incident.

Supplier will provide reasonable assistance with Legends's investigation of the possible Security Incident and any notification obligation of Legends under Applicable Data Protection Laws, such as in relation to individuals or supervisory authorities.

IX. DELETION AND RETURN

Supplier will, within fifteen (15) days of the date of a request from Legends, and in any event within the time period for deletion set out **SCHEDULE 1**, (a) return a copy of all Covered Data Processed by Supplier or any Sub-processors; and (b) delete all other copies of Covered Data Processed by Supplier or any Sub-processors.

X. CONTRACT PERIOD

This DPA will commence on the Effective Date and will remain in effect until terminated by Legends in Legends's sole discretion.

XI. STANDARD CONTRACTUAL CLAUSES

A. The Parties agree that the terms of the Standard Contractual Clauses Module Two (Controller to Processor), as further specified in **SCHEDULE 3** of this DPA, are hereby incorporated by reference and will be deemed to have been executed by the Parties and apply to any transfers of Covered Data from Legends (as data exporter) to Supplier (as data importer) to the extent that:

1. the GDPR applies to Legends when making that transfer; or

2. the transfer is an "onward transfer" (as defined in the Standard Contractual Clauses).

B. Supplier will provide Legends reasonable support to enable Legends's compliance with the requirements imposed on transfers of Covered Data referred to in clause XI(A). Supplier will, upon Legends's request, provide information to Legends which is reasonably necessary for Legends to complete or update its transfer impact assessment ("**TIA**") under Applicable Data Protection Laws.

C. Processer represents, warrants and covenants that: (1) it has not been subject to requests from public authorities for the access to or disclosure of personal data; (2) it has not purposefully created back doors or similar programming that could be used to access its systems and/or Personal Data, (3) it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and (4) that national law or government policy does not require Supplier to create or maintain back doors or to facilitate access to Personal Data or systems or for Supplier to be in possession or to hand over the encryption key.

D. Supplier further agrees to implement the supplementary measures agreed upon and set forth in **SCHEDULE 2** of this DPA in order to enable Legends's compliance with requirements imposed on international transfers of Covered Data under Applicable Data Protection Laws.

XII. DEIDENTIFIED DATA

A. If Supplier receives Deidentified Data from or on behalf of Legends, then Supplier will:

1. take reasonable measures to ensure the information cannot be associated with a Data Subject.
2. publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information.
3. contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

XIII. GENERAL

A. The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

B. Supplier will indemnify, defend and hold harmless Legends and Legends Affiliates against all costs, claims, damages, or expenses incurred by Legends or Legends Affiliates, or for which Legends or Legends Affiliates may become liable due to any failure by Supplier or its personnel, subcontractors, or other agents to comply with any of its obligations under this DPA or the Applicable Data Protection Laws.

C. The Parties agree to negotiate in good faith any amendments to this DPA as may be required in connection with changes in Applicable Data Protection Laws.

D. Except with regard to the Standard Contractual Clauses, this DPA shall be governed by the laws of New York without regard to the choice of law principles thereof, and each of the Parties hereto irrevocably submits to the exclusive jurisdiction of the state and federal courts in New York, New York for the purpose of any suit, action, proceeding, or judgment relating to or arising out of this DPA.

E. If any court or competent authority decides that any term of this DPA is held to be invalid, unlawful, or unenforceable to any extent, such term will, to that extent only, be severed from the remaining terms, which will continue to be valid to the fullest extent permitted by law.

F. Legends's failure to enforce any provision of this DPA will not constitute a waiver of that or any other provision and will not relieve Supplier from the obligation to comply with such provision.

SCHEDULE 1

DETAILS OF PROCESSING

A. List of Parties

The Parties are set out in the preamble to this DPA. With regard to any transfers of Covered Data falling within the scope of the GDPR from Legends to Supplier, additional information regarding the data exporter and data importer is set out below.

1. **Data Exporter**

   The data exporter is: each of the Legends and/or Legends Affiliates

   The data exporter's contact's name and contact details are: Legends GRC Team, dataprivacy@legends.net

   The activities relevant to the data transfer under these Clauses are the receipt and processing of Orders.

2. **Data Importer**

   The data importer is: the Supplier.

   The data importer's contact person and contact details are as provided by Supplier to Legends in writing.

   The data importer's activities relevant to the data transfer under these Clauses are the fulfilment of Orders.

B. Description of Processing

1. **Categories of Data Subjects**

   The categories of Data Subjects whose Personal Data are Processed: *Customers who place orders for Goods that Supplier will assist in fulfilling.*

2. **Categories of Personal Data**

   The Processed categories of Personal Data are: *name, phone number, email address, mailing address, products ordered, date of order, shipping method, product returns (including date, condition and reasons for return).*

3. **Special categories of Personal Data (if applicable)**

   The Processed Personal Data includes the following special categories of data: *N/A*

4. **Frequency of the Processing**

   The Processing is performed: *continuously during the term of this DPA*.

5. **Subject matter and nature of the Processing**

   The subject matter of the Processing is: *order fulfilment services for Legends's Customers, including assisting with returns and responding to Customer inquiries if requested by Legends.*

6. **Purpose(s) of the data transfer and further Processing**

   The purpose/s of the data transfer and further Processing is: *providing order fulfilment services for Legends's Customers, including assisting with returns and responding to Customer inquiries if requested by Legends.*

7. **Storage Limitation**

   The period during which the Personal Data will be Processed, or, if that is not possible, the criteria used to determine that period: *Personal Data will be deleted within ninety (90) days after completion of the applicable Order (as defined in the Agreement) unless otherwise directed by Legends.*

8. **Sub-processor (if applicable)**

For Processing by sub-processors, specify subject matter, nature, and duration of the Processing: *See Schedule 4. Processing by Sub-processors occurs continuously while the Agreement remains in place.*

C. Competent Supervisory Authority

The competent supervisory authority is the supervisory authority of Spain.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

Supplier represents, warrants and covenants that Supplier has implemented the following technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

1) Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Supplier's information security program.

2) Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Supplier's organization, monitoring and maintaining compliance with Supplier's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3) Utilization of commercially available and industry standard encryption technologies for Covered Data that is:

a) being transmitted by Supplier over public networks (i.e., the Internet) or when transmitted wirelessly; or

b) at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).

4) Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

5) Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Supplier's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Supplier's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6) System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

7) Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (a) protect information assets from unauthorized physical access, (b) manage, monitor, and log movement of persons into and out of Supplier facilities, and (c) guard against environmental hazards such as heat, fire, and water damage.

8) Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Supplier's possession.

9) Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Supplier's technology and information assets.

10) Incident / problem management procedures design to allow Supplier to investigate, respond to, mitigate, and notify of events related to Supplier's technology and information assets.

11) Network security controls that provide for the use of firewall systems, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12) Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

13) Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

14) Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of formal or informal requests from public authorities to access the data.

15) Development of specific training procedures for personnel in charge of managing requests for access to Personal Data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.

16) Adoption of strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures. Such policies and practices shall include data minimization where appropriate to limit the exposure of Personal Data to unauthorized access.

17) Development and implementation of best practices to appropriately and timely involve and provide access of information to the personnel of Supplier responsible for international transfers of Personal Data.

18) Adoption and regular review by Supplier of internal policies to assess the suitability of the implemented measures and identify and implement additional or alternative solutions when reasonable to ensure that the Covered Data is sufficiently protected.

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

1. **EU SCCS**

The Standard Contractual Clauses will apply to any Processing of Covered Data that is subject to the GDPR. For the purposes of the Standard Contractual Clauses:

1.1 Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

1.2 Clause 9(a) option 2 (General written authorization) is selected, and the time period to be specified is determined in clause V(C) of the DPA.

1.3 The option in Clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.

1.4 With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that, option 1 will apply and the governing law will be the law of Spain.

1.5 In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of Spain.

1.6 For the purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority

1.7 For the purpose of Annex II of the Standard Contractual Clauses, Schedule 2 of the DPA contains the technical and organizational measures.

2. **UK ADDENDUM**

2.1 This paragraph 2 (the "**UK Addendum**") shall apply to any transfer of Covered Data from Legends (as data exporter) to Supplier (as data importer) to the extent that: (a) the UK GDPR applies to Legends when making that transfer; or (b) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this UK Addendum:

“Approved Addendum” means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Mandatory Clauses.

“Mandatory Clauses” means “Part 2: Mandatory Clauses” of the Approved Addendum.

2.3 2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum

2.4 The Approved Addendum shall be deemed completed as follows:

(a) the "Addendum EU SCCs" shall refer to the Standard Contractual Clauses as they are incorporated into this Agreement in accordance with clause XI and this Schedule 3;

(b) Table 1 of the Approved Addendum shall be completed with the details in paragraph A of Schedule 1;

(c) the "Appendix Information" shall refer to the information set out in Schedule 1 and Schedule 2

(d) for the purposes of Table 4 of the Approved Addendum, Legends (as data exporter) may end this DPA, to the extent the Approved Addendum applies, in accordance with Section 19 of the Approved Addendum; and

(e) Section 16 of the Approved Addendum does not apply.

3. **SWISS ADDENDUM**

3.1 This Swiss Addendum will apply to any Processing of Covered Data that is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR.

3.2 **Interpretation of this Addendum**

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

"**Addendum**" means this addendum to the Clauses;

"**Clauses**" means the Standard Contractual Clauses as incorporated into this DPA in accordance with clause XI and as further specified in this Schedule 3;

"**FDPIC**" means the Federal Data Protection and Information Commissioner; and

"**Swiss Data Protection Laws**" means the Swiss Federal Act Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force for time to time.

(b) This Addendum shall be read and interpreted in a manner that is consistent with Swiss Data Protection Laws, and so that it fulfils the Parties' obligation to provide appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(c) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) 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, re-enacted and/or replaced after this Swiss Addendum has been entered into.

(e) In relation to any Processing of Personal Data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends and supplements the Clauses to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter’s Processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

3.3 **Hierarchy**

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 **Changes to the Clauses for transfers exclusively subject to Swiss Data Protection Laws**

(a) To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.3(a)) the following amendments are made to the Clauses:

(i) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(ii) Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter’s Processing when making that transfer."

(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or "“GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

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

(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

(vii) Clause 17 is replaced to state

"These Clauses are governed by the laws of Switzerland".

(viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws will be resolved by the courts of Switzerland. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

(ix) Until the entry into force of the revised Swiss Data Protection Laws, the Clauses will also protect Personal Data of legal entities and legal entities will receive the same protection under the Clauses as natural persons.

3.5 **Supplementary provisions for transfers of Personal data subject to both the GDPR and Swiss Data Protection Laws**

(a) To the extent that the data exporter's Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" under both the Clauses and the Clauses as amended by paragraph 3.3(c) of this Addendum:

(i) for the purposes of Clause 13(a) and Part C of Annex I:

(A) the FDPIC shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer, or such transfer is an "onward transfer" as defined in the Clauses (as amended by paragraph 3.3 of this Addendum; and

(B) subject to the provisions of paragraph 2 of this Schedule 3 (UK Addendum), the supervisory authority identified in Schedule 1 shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent the GDPR applies to the data exporter's processing, or such transfer is an "onward transfer" as defined in the Clauses.

(ii) the terms "European Union", "Union", "EU", and "EU Member State" shall not be interpreted in a way that excludes the ability of Data Subjects in Switzerland bringing a claim in their place of habitual residence in accordance with Clause 18(c) of the Clauses; and

(iii) Until the entry into force of the revised Swiss Data Protection Laws, the Clauses will also protect Personal Data of legal entities and legal entities will receive the same protection under the Clauses as natural persons.

SCHEDULE 4

SUB-PROCESSORS

Name of Sub-processor	**Description of Processing**
Amazon Web Services	*Cloud computing services*
Google Cloud Platform	*Cloud computing services*