CONFIDENTIAL

Data Protection Addendum (Data Controller to Data Controller)

Recitals

The Data Protection Addendum (the "DPA") is incorporated as part of the master agreement ("Agreement") made between the Supplier/ Distributor/ Agency ("Partner") and Hong Kong Express Airways Limited ("UO") (collectively, "Parties").

This DPA governs the processing of Personal Data that the Partner transfers or otherwise provides UO (or vice versa) in connection with the performance of the agreement and sets out additional rights and obligations of the Parties, which apply when the Partner and UO each acts as a Controller in respect of the Personal Data.

Applicable DPA Terms

When the Partner enters into the Agreement with UO, the then-current DPA terms will apply and will not change during the term of the Agreement. For the avoidance of doubt, when the Partner renews or varies the Agreement, the then most updated DPA terms will apply to the renewal or variation of the Agreement during the renewed term of the Agreement.

Prior Versions

For earlier versions of the DPA, the Partner may contact its UO contact for the Agreement.

NOW, THEREFORE, the Parties agree as follows:

1. Effective date

This Addendum shall take effect between UO and the Partner and become legally binding on the Parties on the date the Agreement is signed.

2. Obligations of the Parties

(a) Each Party undertakes to Process Personal Data which it receives from the other Party (including, where applicable, Affiliates of the other Party in accordance with Applicable Privacy Laws. Without limiting the foregoing, each Party shall take reasonable measures to ensure protection of the rights of Data Subjects and security and confidentiality of the Personal Data Processed, including without limitation, by introducing and maintaining internal organisational and security measures and by ensuring the lawfulness of the Processing (including collecting the appropriate Consent, if required under Applicable Privacy Laws). For the purposes of this Addendum, the reference to UO shall include any Affiliates of UO to the extent any Personal Data is disclosed by Affiliates of UO.

(b) Each Party shall ensure Data Subjects are provided with relevant information about the transfer of Personal Data to the other Party, including the provision of notice that Personal Data will be Processed by such other Party for the purposes contemplated by the arrangements between the Parties under the Agreement.

(c) The Partner shall promptly notify UO if any adverse development arises (including a change of control of the Partner, change of Applicable Privacy Laws to which the Partner is subject, or any force majeure event) which, in the Partner's reasonable opinion, is likely to result in the Partner being unable to perform its obligations under this Addendum, and co-operate with UO in good faith in order to mitigate the effects that may be caused by such adverse development.

(d) The Partner shall not use any Automated Decision Making in Processing the Personal Data without the express written consent of UO.

(e) The Partner shall not, without UO's prior written consent, transfer any Personal Data provided by UO to any third party (including any entity within the Partner's group of companies) located outside the jurisdiction where the Partner is located at. UO hereby consents that the Partner may transfer Personal Data provided by UO to the entities listed in Schedule A.

(f) Schedule A sets out certain information regarding the Processing of Personal Data by the Parties.

3. Data Subject Requests and other complaints and requests

(a) Without limiting the Partner's obligations under this clause 3, the Parties acknowledge that: (i) Data Subjects are granted certain Data Subject rights under the Applicable Privacy Laws which may be exercised in respect of both the Partner and UO; and (ii) the Partner and UO may be liable in respect of breaches of such Data Subject rights.

(b) Each Party must, to the extent permitted by Applicable Privacy Laws, promptly notify the other Party if it receives a Data Subject Request in respect of any Personal Data Processed by the other Party which may impact the other party's Processing of the Personal Data or assistance from the other Party may be required.

(c) Each Party will provide the other Party with such assistance and co-operation as it reasonably requests to enable the requesting Party to comply with any obligations imposed on it by Applicable Privacy Laws in relation to the Processing of Personal Data. A Party will be entitled to refuse or limit its assistance where the requesting Party is in the position to fulfil the obligations without the other Party's assistance.

4. Security

Each Party must take, and must ensure it takes, all appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of systems used for Processing of Personal Data and protect against the unlawful destruction, loss, alteration, unauthorised disclosure of or access to the Personal Data transmitted, stored or otherwise Processed as defined in Schedule B to this Addendum.

5. Security Breach Management and Notification

(a) Each Party must notify the other Party immediately upon becoming aware of the occurrence of any incident which has resulted, or is reasonably likely to result, in any accidental or unlawful loss, theft, tampering, access, use, deletion, disclosure or corruption of Personal Data and / or any unauthorised use or access to Personal Data (a **Security Incident**).

(b) In the event of a Security Incident, the Party experiencing the Security Incident shall promptly take adequate remedial measures.

(c) Each Party must provide all such cooperation and information reasonably requested by the other Party on an ongoing basis to assist in the investigation, mitigation and remediation of a Security Incident, including providing regular updates to the other Party in respect of the Security Incident.

(d) Unless otherwise required by law, the Party experiencing the Security Incident shall not communicate details of a Security Incident to any Regulator, Data Subjects and / or the media without the other Party's prior written consent, which shall not be unreasonably withheld.

6. Cooperation with Regulators

(a) Each Party must promptly notify the other Party of all enquiries from a Regulator which relates to the other Party's Processing of Personal Data, or to the other Party's obligations under the Agreement and/or this Addendum, unless prohibited from doing so at law or by a Regulator.

(b) Where requested by either party, and only to the extent required by Applicable Privacy Laws or a Regulator which the requesting Party is subject to, the other Party must cooperate with, and comply with all reasonable requests or directions by, the Party to enable it to verify and / or procure that the other Party is in full compliance with its data protection obligations under the Agreement and this Addendum, including making available all information necessary to demonstrate such compliance. For the purposes of this clause 6(b), the Partner shall, and shall procure its Processors to, maintain complete and accurate records of its respective data Processing activities, such records to be maintained for a minimum of three (3) years.

7. Restricted Transfer

(a) If, in the performance of the relevant obligations under the Agreement:

(i) a Restricted Transfer shall be made with respect to Personal Data originating in the EEA, and the transfer is not subject to an adequacy determination by the European Commission, the Parties agree that the Module 1 of Standard Contractual Clauses will apply (Schedule C) and are deemed to have signed such Standard Contractual Clauses;

(ii) a Restricted Transfer shall be made with respect to Personal Data originating in the UK, and the transfer is not subject to any adequacy regulations by UK GDPR, the Parties agree that, the Standard Contractual Clauses (Schedule C) and the UK Addendum (Schedule D) will apply and are deemed to have signed such Standard Contractual Clauses and the UK Addendum; and

(iii) a Restricted Transfer shall be made with respect to Personal Data originating in jurisdictions other than the EEA and the UK such Restricted Transfer shall be made by way of the relevant standard contractual clauses or other applicable data transfer mechanisms as permitted under Applicable Privacy Laws.

(b) With respect to any Restricted Transfers, such Restricted Transfer shall be made in compliance with Applicable Privacy Laws. Prior to making any Restricted Transfer beyond jurisdictions set out in Schedule A, the Partner shall notify UO of the name and location (territory or country) of the recipient, as well as the reason and appropriate data transfer mechanism in place for the Restricted Transfer.

(c) The Partner acknowledges that, in the event it transfers Personal Data pursuant to the Agreement (including to Processors), it will undertake any corresponding data transfer impact assessment or a third party privacy assessment so as to identify and implement any proportionate legal, technical and operation safeguards (including privacy by design and by default measures, where necessary) to protect against the loss, disclosure or access of any Personal Data and as otherwise required under Applicable Privacy Laws.

8. General

8.1 Third Party Claims

(a) In its capacity as independent Controllers, each Party shall remain fully and solely responsible to the Data Subjects for the Processing of Personal Data which it has in its possession, including without limitation, in relation to any claim for compensation made by a person who has suffered material or moral damage as a result of its violation of Applicable Privacy Laws.

(b) In the event a Data Subject makes any claim, complaint, demand, suit, action or proceeding (**Claim**) against a Party as a result of the Processing of Personal Data undertaken by the other Party, the first-mentioned Party shall promptly give the other Party notice of the details and nature of the Claim and the other Party shall take control of the Claim including without limitation, to promptly confirm to the Data Subject its actual role as Controller with regard to the Processing of the Personal Data of the Data Subject.

8.2 Liability

The Parties agree that no limitations of liability set out in the Agreement will apply to any Party's liability arising under or in connection with this Addendum, including without limitation, under Clause 8.1.

8.3 Exclusion of third-party rights

The Parties acknowledge and agree that Data Subjects may be granted third-party rights under the Standard Contractual Clauses and the UK Addendum and/or Applicable Privacy Laws. Except in respect of any rights or benefits conferred to Affiliates of a Party which shall be enforceable by them as against the other Party, all other third-party rights are excluded.

8.4 Governing Law

Except to the extent required by the Standard Contractual Clauses (incorporated in Schedule C) and the UK Addendum (incorporated in Schedule D) this Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

8.5 Order of precedence

(a) Partner's obligations under this Addendum are in addition to and not in lieu of its obligations under any other provisions of the Agreement. If there is an inconsistency between this Addendum and any other part of the Agreement, the terms of this Addendum shall apply unless the variations to the terms of this Addendum have been expressly agreed in the Agreement.

(b) To the extent that the Standard Contractual Clauses and the UK Addendum are applicable, if there is an inconsistency between the Agreement and the Standard Contractual Clauses (incorporated in Schedule C) and the UK Addendum (incorporated in Schedule D, the Standard Contractual Clauses and the UK Addendum will prevail to the extent of that inconsistency.

8.6 Changes in Applicable Privacy Laws

(a) If any variation is required to this Addendum as a result of a change in Applicable Privacy Laws, then either Party may provide written notice to the other Party with respect to such change in Applicable Privacy Laws.

(b) On receipt of a notice under clause 8.6(a), the Parties shall discuss the change in Applicable Privacy Laws and negotiate in good faith with a view to agreeing any necessary variations to this Addendum and executing any additional appropriate documentation and safeguards, in order to address such changes in Applicable Privacy Laws.

8.7 Counterparts

This Addendum may be executed in any number of counterparts. All counterparts together will be taken to constitute one instrument.

8.8 Notices

All notices, requests, demands and determinations under this Addendum (other than routine operational communications), and notably all notifications under clause 3 of this Addendum, shall be in writing and, in addition to complying with the notice provisions as set out in the Agreement, shall also be sent to the data protection officer, should such have been designated in accordance with Article 37 of the GDPR, or any other Personnel in charge of protection of Personal Data for the Party to the following addresses:

For UO:	For Partner:
Contact name: Data Protection Officer	Contact name: as listed in the Agreement
E-mail: dpo@hkexpress.com	Email: as listed in the Agreement

8.9 Structure of the Addendum, definitions and interpretation

(a) This Addendum consists of:

(i) the main body of this Addendum, being clauses 1 to 9;

(ii) Schedule A (Personal Data Processing Details);

(iii) Schedule B (Technical and Organisational Measures including Technical and Organisational Measures to ensure the security of the Data);

(iv) Schedule C (the Standard Contractual Clauses); and

(v) Schedule D (International Data Transfer Addendum to the Standard Contractual Clauses).

(b) In this Addendum, except where the context otherwise requires:

(i) unless the contrary intention appears, or a term is otherwise defined in this Addendum, a term defined in the Agreement has the same meaning in this Addendum;

(ii) a reference to this Addendum includes any attachment to it, as amended by the Parties in writing.

(c) In this Addendum:

Affiliates of a Party means:

(a) branch offices of that Party; and

(b) an entity which (directly or indirectly) controls, is controlled by or is under common control with, that Party, where control refers to the power to direct or cause the direction of the management policies of another entity, whether through ownership of voting securities, by contract or otherwise.

Agreement has the meaning given to it in the Recitals of this Addendum and includes this Addendum as incorporated under the Agreement.

Applicable Privacy Laws means all laws and regulations applicable to the Processing of Personal Data under the Agreement including the EU GDPR, UK GDPR, Chinese Mainland Data Protection Laws, the PDPO, and the privacy policy issued by UO from time to time and any other applicable principles, industry codes and policies that may be applicable to the Processing of Personal Data, in each case as amended or supplemented from time to time.

Automated Decision Making means the activity of using computer programs to automatically analyse or assess personal behaviours, habits, interests, hobbies or financial, health, credit or other status, and make decisions based upon the foregoing activity.

Chinese Mainland means the mainland of the People's Republic of China, and excludes, for the purposes of this Addendum, Hong Kong SAR, Macau SAR and Taiwan.

Chinese Mainland Data Protection Laws means the Personal Information Protection Law of the Chinese Mainland, Data Security Law of the Chinese Mainland, Cybersecurity Law of the Chinese Mainland, Personal Information Security Specifications, and any other legislation, administrative rules, regulations, measures and regulatory guidelines as issued from time to time, in each case which may be applicable to the Processing of Personal Data.

Claim is defined in clause 8.1(b).

Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Data Subject Request means a Data Subject's request to exercise that Data Subject's rights under Applicable Privacy Laws in respect of that Data Subject's Personal Data, including, without limitation, the right to access, correct, amend, transfer, obtain a copy of, object to the Processing of, block or delete such Personal Data.

EEA means the European Economic Area, which as at the date of this Addendum, comprises the European Union member states, Iceland, Liechtenstein and Norway.

EU GDPR means the EU General Data Protection Regulation 2016/679.

GDPR means each of EU GDPR, UK GDPR or both together (as the context requires).

Party means either UO and the Partner and **Parties** mean both of them collectively.

PDPO means the *Personal Data (Privacy) Ordinance (Cap. 486)* as amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 of the Hong Kong Special Administrative Region.

Personal Data means any Personal Data Processed by any of the Party pursuant to or in connection with the Agreement.

Personnel, in relation to a Party, means that Party's officers, employees, contractors or agents, including employees or independent contractors of such contractors or agents.

Regulator means the data protection authority or other regulatory or governmental bodies or Supervisory Authority (including any certified or authorised bodies which are appointed by such authorities) with authority over all or any part of: (a) the Processing of Personal Data in connection with the Agreement; or (b) a Party's business or Personnel.

Restricted Transfer means (a) a transfer of Personal Data (which is being Processed under this Agreement) to a Third Country; and (b) where applicable under Applicable Privacy Laws, permitting remote access to Personal Data from a Third Country.

Third Country means a country, territory or organisation that is not recognised under Applicable Privacy Laws as providing adequate protection in respect of the Personal Data.

Security Incident is defined in clause 5(a).

Standard Contractual Clauses means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

UK means the United Kingdom, comprising England and Wales, Scotland, or Northern Ireland.

UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0) issued by the ICO under s119A(1) of the UK Data Protection Act 2018, in force from 21 March 2022.

UK GDPR means the EU General Data Protection Regulation 2016/679 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data as it forms part of the law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018, and includes any amendment made to it by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", **"Processor"**, "**Processing**" and "**Supervisory Authority**" have the same meaning as in the GDPR, and shall be equivalent to the corresponding terms which are adopted under Applicable Privacy Laws (other than the GDPR), and their other grammatical forms shall have a corresponding meaning.

9. Legal Effect

This Addendum, and the Standard Contractual Clauses and the UK Addendum incorporated within this Addendum, shall take effect between, and become legally binding between the Parties, on the date the Agreement is signed.

SCHEDULE A

This Schedule A includes certain details of the Processing of Personal Data.

A. LIST OF PARTIES

Data exporter(s):

1. Name: HONG KONG EXPRESS AIRWAYS LIMITED
2. Address: 1st Floor, 11 Tung Fai Road, Hong Kong International Airport, Lantau, Hong Kong
3. Contact person's name, position and contact details: Data Protection Officer, DPO@hkexpress.com
4. Activities relevant to the data transferred under these Clauses: The performance of the Agreement
5. Signature and date: The Parties are deemed to agree to follow the Standard Contractual Clauses by executing the Agreement and the date shall be the execution date of the Agreement.
6. Role (controller/processor): controller

Data importer(s): Name: as listed in the Agreement

1. Address: as listed in the Agreement Contact person's name, position and contact details: as listed in the Agreement
2. Activities relevant to the data transferred under these Clauses: The performance of the Agreement
3. Signature and date: The Parties are deemed to agree to follow the Standard Contractual Clauses by executing the Agreement and the date shall be the execution date of the Agreement.
4. Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

Item No.	Data requirement	Details of the Processing of Personal Data
1	**Subject matter and duration of the Processing of Personal Data**	The subject matter and duration of the Processing of Personal Data are set out in the Agreement and this Addendum.
2	**The nature and purpose of the Processing of Personal Data**	The nature and purpose of processing is for the performance of the Agreement.
3	**The types of Personal Data to be Processed**	Both UO and Partner may Process the Personal Data from any of the following categories, to the minimum extent necessary for the purpose as stated in item 2 above: (a) name (first name, middle name(s) and surname), birth name, maiden name or any additional names, address, title, preferred salutation; (b) business contact information (company, telephone number, email address, business address), personal contact information (company, telephone number, email address, address), social media username or alias and other contact information; (c) professional life data including occupation, employer, employment status, income, and other occupation or income related data;

Item No.	Data requirement	Details of the Processing of Personal Data
		(d) personal life data including marital status, lifestyle, hobbies and interests, and other background data and relationship management information; (e) unique account or customer numbers, or other internal identifiers; (f) bank account numbers, names and transaction descriptions, along with other transaction details; (g) your employee numbers or other of your internal identifiers and names, job titles and email address; (h) instant message or live chat logs; (i) meeting, telephone or attendance notes, emails, letters or other data relating to communications, calls and meetings; (j) ongoing monitoring data in connection with compliance and / or fraud prevention; (k) IP address, browser generated information, device information, geo-location markers and other digital identifiers used for tracking, profiling or location purposes; (l) end-user usage information of UO's online and / or mobile applications; and (m) other metadata relating to the use of UO's systems and applications.
4	**The types of special categories of Personal Data to be Processed**	As listed in the Agreement, if any.
5	**The categories of Data Subject to whom Personal Data relates**	Both UO and Partner may process Personal Data of the Data Subjects from any of the following categories, to the minimum extent necessary for the purpose as stated in item 2 above: (a) current, prospective and former clients and customers of UO (UO Clients) and employees, agents, advisors and other authorised representatives of UO Clients; (b) suppliers, subcontractors, vendors and business partners of UO (Third Parties) and employees, agents, advisors, and other authorised representatives of Third Parties; (c) users authorised by UO to use the Services (Authorised Users) and any employees, agents, advisors and other authorised representatives of Authorised Users; (d) visitors to UO's websites and persons connecting, or attempting to connect or gain access to UO's network or systems; (e) current, prospective and former employees, contractors, agents, officers, directors and other representatives of UO (Staff); (f) relatives, dependents and beneficiaries of Staff; and (g) professional advisors and consultants to UO.

Item No.	Data requirement	Details of the Processing of Personal Data
6	**UO's obligations and rights**	UO's obligations and rights as the Controller are set out in the Agreement.
7	**Retention Period**	Personal Data to be retained may be retained by the Contracted Processors from the date of the Agreement until the expiry / termination of the Agreement.
8	**Cross-border transfer of Personal Data**	The Parties agree Personal Data may be transferred to the following countries and regions (including countries and regions from which Personal Data may be remotely accessed or transited through): • worldwide
9	**Subprocessors**	• Please refer to sub-processors approved by UO in the Agreement and/or other documentation agreed between the Parties.

SCHEDULE B

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

1. The Partner must comply with the following Information Security Requirements in relation to the UO Data it receives (and in the event of any conflict between any of the Information Security Requirements below, the most stringent or the highest level of security standard shall apply):

(a) take all appropriate physical, technical and organisational security measures and observe Good Industry Practice to protect UO Data, in particular against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to any UO Data transmitted, stored or otherwise Processed. This shall include measures to ensure the ongoing confidentiality, integrity, availability and resilience of the UO Systems, and the ability to restore the availability and access to UO Data in a timely manner in the event of a physical or technical security incident;

(b) in respect of any environments which accesses, stores or processes UO Data, at all times establish and maintain a security environment which complies with the following international standards for information security and must provide annual attestations and certification of compliance for each of the following to UO:

(i) the ISO/IEC 27001- Information Security Management Systems - Requirements; and/ or

(ii) the National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1; and/or

(iii) International Standards on Assurance Engagement No. 3402 (ISAE 3402) - Service Organisation Control 2 (SOC 2) Type II; and/or

(iv) Other standards as agreed by the Parties.

(c) to the extent the Partner processes cardholder data, at all times establish and maintain a security environment which complies with the Payment Card Industry Data Security Standard (PCI-DSS) (and must provide annual attestations and certification of compliance of such standard to UO);

(d) establish and maintain formal documentation, policies and practices addressing the security requirements referred to above in sub-paragraph (ii) and the following additional requirements (with such documentation to be approved by an appropriate level of management on an annual basis):

(i) secure access controls (i.e. users are assigned with unique user IDs with clear ownership which are traceable to an individual, the processing systems must be enforced with complex passwords and Multi-Factor authentication to prevent any unauthorized access.);

(ii) encryption protocols in respect of all storage devices and systems:

(A) for data at rest, using AES-256 (at a minimum); and

(B) for data in transit, using file level encryption with AES-256 (at minimum) for transmission via email and using TLS 1.2 (at a minimum) for transmission via network connections; and

(iii) malware and vulnerability management, including conducting at least annual penetration testing on all external or internet facing systems; and

(e) comply with UO's information security standards as provided by UO in writing from time to time,

("**Information Security Requirements**").

2. In this Schedule B:

UO Data means any data relating to any business of UO, including its operations, facilities, customers, employees, assets, products, sales and transactions, in whatever form the data exists, and includes any database in which data or information is contained; documentation or records related to data or information; and copies of any of the above.

UO System means any computer or other system owned or operated by UO.

Good Industry Practice means that degree of skill, diligence, prudence, care, foresight and practice which would reasonably and ordinarily be expected of a skilled and experienced provider engaged in the same or a similar type of business as that of the Partner (within the aviation sector or otherwise) under similar circumstances.

SCHEDULE C

MODULE 1 OF STANDARD CONTRACTUAL CLAUSES

The parties agree that the following terms apply:

(i) the Irish Supervisory Authority (i.e. The Data Protection Commission of Ireland) shall be the competent Supervisory Authority pursuant to Clause 13 of the Standard Contractual Clauses;

(ii) data subjects for whom an entity processes EU Personal Data are third-party beneficiaries under the Standard Contractual Clauses;

(iii) the Standard Contractual Clauses shall be governed by the law of Ireland, which allows for third-party beneficiary rights pursuant to Clause 17 of Standard Contractual Clauses; and

(iv) any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of Ireland pursuant to Clause 18 of Standard Contractual Clauses.

(v) Schedule A to this DPA shall apply as Annex I of Standard Contractual Clauses and Schedule B shall apply as Annex II of Standard Contractual Clauses.

SCHEDULE D

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES ("EU SCCs")

Part 1: Tables

Table 1: Parties

Start date	**The signing date of the Agreement**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: HONG KONG EXPRESS AIRWAYS LIMITED Main address (if a company registered address): 1st Floor, 11 Tung Fai Road, Hong Kong International Airport, Lantau, Hong Kong Official registration number (if any) (company number or similar identifier): 19325407	Full legal name: as listed in the Agreement Trading name (if different): as listed in the Agreement Main address (if a company registered address): as listed in the Agreement Official registration number (if any) (company number or similar identifier): as listed in the Agreement
Key Contact	Full Name (optional): Job Title: Data Protection Officer Contact details including email: dpo@hkexpress.com	Full Name (optional): Job Title: as listed in the Agreement Contact details including email: as listed in the Agreement
Signature (if required for the purposes of Section 2)	The Parties are deemed to agree to follow the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses by executing the Agreement and the date shall be the execution date of the Agreement.	The Parties are deemed to agree to follow the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses by executing the Agreement and the date shall be the execution date of the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	×	×	Excluded			

Table 3: Appendix Information

"**Appendix Information**" means 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 1A: List of Parties: See item A of Schedule A
Annex 1B: Description of Transfer: See item B of Schedule A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule B – "Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data".
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party

Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.