CONFIDENTIAL

DATA PROTECTION ADDENDUM (CONTROLLER TO PROCESSOR)

Recitals

The Data Protection Addendum (the "DPA") is incorporated as part of the master agreement ("Agreement") made between UO's vendor, hotel or travel agent, ground services provider, lounge operator and other business partner such as credit card partners and insurance partners ("Supplier") and Hong Kong Express Airways Limited ("UO") (collectively, "Parties").

This DPA governs the processing of Personal Data that UO may, from time to time, share or transfer Personal Data (e.g., passenger details, passenger travel or hotel stay information, loyalty program information, payment information, insurance details) of our customers (in other words, "Data Subjects") with the Supplier, or may grant these third parties access to Personal Data, in connection with the performance of the agreement and sets out additional rights and obligations of the Parties, which apply when UO acts as a Controller and the Supplier acts as a Processor in respect of the Personal Data.

Applicable DPA Terms

When the Supplier 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 Supplier 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 Supplier 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 Supplier and become legally binding on the Parties on the date the Agreement is signed.

2. **Processing of UO Personal Data**

(a) The Parties agree that UO and/or, where applicable, the Affiliates of UO are the Controller of UO Personal Data and that the Supplier will Process UO Personal Data on behalf of UO as its Processor. For the purposes of this Addendum, the reference to UO shall include any Affiliates of UO to the extent any UO Personal Data is disclosed by Affiliates of UO to the Supplier.

(b) Except as otherwise agreed in the Agreement in writing, UO instructs the Supplier to Process UO Personal Data to the extent necessary for the provision of Products and/or Services and in a manner consistent with the Agreement and for the purpose and extent described in Annex A of this Addendum.

(c) The Supplier must:

(i) comply with all Applicable Privacy Laws in the Processing of UO Personal Data;

(ii) not Process UO Personal Data other than on UO's documented instructions (including this Addendum), unless Processing of UO Personal Data is required to comply with the relevant law to which the Supplier is subject, in which case the Supplier shall promptly inform UO of that legal requirement prior to such relevant Processing of UO Personal Data, unless such law prohibits notice to UO;

(iii) notify UO immediately if, in the Supplier's reasonable opinion, the Supplier believes that any suspected or actual breach of this Addendum or any documented instructions issued by UO infringe any Applicable Privacy Laws;

(iv) not provide the Products and/or Services in a manner that causes UO to violate any Applicable Privacy Laws;

(v) notify UO immediately if any adverse development arises (including a change of control of the Supplier, change of Applicable Privacy Laws to which the Supplier is subject, or any force majeure event) which, in the Supplier's reasonable opinion, is likely to result in the Supplier 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;

(vi) not transfer, and not make any Restricted Transfers in relation to, any UO Personal Data to any region or territory other than on UO's documented instructions (in which case, the restrictions set out in clause 9 shall apply) and in accordance with the Applicable Privacy Laws;

(vii) put in place adequate measures to ensure that any Personal Data in its possession or control remain accurate and complete, and upon request by UO, take steps to correct any errors in the Personal Data; and

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

(d) Annex A sets out certain information regarding the Supplier's Processing of UO Personal Data.

3. **Data Subject Requests and other complaints and requests**

(a) Without limiting the Supplier'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 Supplier and UO; and (ii) the Supplier and UO may be liable in respect of breaches of such Data Subject rights.

(b) The Supplier must, unless otherwise prohibited by law, promptly (and in any event within 72 hours) notify UO if a Contracted Processor receives a Data Subject Request in respect of or in connection with any UO Personal Data. The Supplier must not, and must ensure that each Subprocessor does not, respond to any such Data Subject Request without UO's prior written instructions.

(c) The Supplier must provide such assistance and take such action as UO may reasonably request (including assistance by appropriate technical and organisational measures) to allow UO to fulfil its obligations under Applicable Privacy Laws in respect of Data Subject Requests, including meeting any statutory deadlines imposed by such obligations.

(d) The Supplier must, unless otherwise prohibited by law, promptly notify UO upon receipt of any complaint or request (other than Data Subject Requests or enquiries of Regulators described in clause 10) relating to:

(i) UO's obligations under Applicable Privacy Laws; or

(ii) UO Personal Data,

and shall promptly provide such reasonable cooperation and assistance as UO may request in relation to such complaint or request. The Supplier shall not, and shall ensure that each Subprocessor does not, respond to any such complaint or request without UO's prior written instructions.

4. **Supplier's Personnel**

The Supplier must ensure that the Personal Data is only accessible to personnel of any Contracted Processor who have a need to access such Personal Data in order to carry out their roles in the performance of the Supplier's obligations under the Agreement. Personnel of any Contracted Processor engaged in the Processing of UO Personal Data must be informed of the confidential nature of UO Personal Data, have received appropriate training on their responsibilities (including not to Process UO Personal Data except to the extent necessary to provide the Products and/or Services) and have executed written confidentiality agreements no less stringent than the confidentiality obligations set out under this Addendum in respect of the UO Personal Data that survive termination of the engagement of the personnel.

5. **Subprocessors**

(a) UO consents to the Supplier engaging Subprocessors to Process UO Personal Data to the extent necessary for the provision of the Products and/or Services, subject to clauses 5(b) to (e) and the other provisions of the Agreement.

(b) Where the Supplier engages a Subprocessor, the Supplier must ensure prior to the Processing taking place, that the Supplier has provided UO with such information regarding the Subprocessor as UO may require and that the arrangement between the Supplier and the Subprocessor is governed by a written agreement that specifies the Subprocessor's Processing activities and imposes on the Subprocessor the same or stricter terms as those imposed on the Supplier in this Addendum. The Supplier will procure that Subprocessors will perform all obligations set out in this Addendum.

(c) UO consents to the Supplier's use of Subprocessors listed in the Agreement (**Subprocessor List**) to Process the UO Personal Data as set out in Annex A to the extent necessary for the provision of the Products and/or Services, subject to the Supplier's compliance with the terms of this Addendum and in particular clause 5(b) above. The Supplier will not make changes to the Subprocessor List without UO's prior written consent. Without limitation to the foregoing, if the Supplier intends to change any Subprocessor (such as an addition or replacement), the Supplier shall provide sixty (60) days' prior written notice by email to UO before the proposed change is due to take effect, providing UO with the opportunity to consent or object to the change of, or any addition of a new Subprocessor to the Subprocessor List. Upon request, the Supplier shall promptly provide UO with the current Subprocessor List.

(d) UO will notify the Supplier of its consent or objection to the proposed change no later than 10 days before the proposed change is due to take effect. No change will come into effect unless and until UO has notified the Supplier in writing of its consent to such change. If UO objects in writing to the Supplier's proposed use of a new Subprocessor, the Supplier will refrain from permitting such proposed Subprocessor to Process UO Personal Data without adversely impacting the Products and/or Services or UO. If the Supplier determines that it cannot avoid such an adverse impact despite its reasonable efforts, the Supplier shall notify UO of such determination. Upon receipt of such notice, UO may terminate all or any part of the Agreement without penalty or liability (other than for fees due and owing to the

Supplier for Products and/or Services performed prior to such termination) effective immediately upon written notice of such termination to the Supplier. The Supplier shall refund UO any prepaid fees for the period following the effective date of termination.

(e) The Supplier will be responsible and liable for the acts, omissions or defaults of its Subprocessors in connection with the Agreement (including this Addendum), as if they were the Supplier's own acts, omissions or defaults.

6. **Security**

The Supplier must take, and must ensure that each Contracted Processor takes, all appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of systems used for the Processing of UO Personal Data and to ensure a level of security appropriate to the risk presented by the Processing of UO Personal Data, and protect against the unlawful destruction, loss, alteration, unauthorised disclosure of or access to UO Personal Data transmitted, stored or otherwise Processed. The Supplier must promptly notify UO of any changes to its technical and organisational measures which may affect the Processing of UO Personal Data.

7. **Audits**

(a) The Supplier shall, and shall procure its Subprocessors to, maintain complete and accurate records of its respective data Processing activities, such records to be maintained for a minimum of three (3) years.

(b) Where requested by UO, the Supplier must:

(i) permit UO (or its nominated personnel) to inspect and audit the Supplier's data Processing activities (and / or those of its agents and / or Subprocessors which Process UO Personal Data);

(ii) cooperate with, contribute to and comply with all reasonable requests or directions by, UO to enable it to verify and/or procure that the Supplier 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; and

(iii) take such remedial actions as are reasonably required by UO following such audit.

(c) Where requested by UO, unless prohibited by applicable law, the Supplier must provide UO with such assistance and information as may be reasonably required in order for UO to comply with any obligation under Applicable Privacy Laws.

8. **Security Breach Management and Notification**

The Supplier must:

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

(b) provide all cooperation and information reasonably requested by UO on an ongoing basis to assist in the investigation, mitigation and remediation of in respect of a Security Incident, including, as soon as possible following, and in any event within 48 hours of, the detection of the Security Incident by the Supplier (or such earlier timeframe as required by a Regulator):

(i) full details of the Security Incident, including the categories and approximate number of Data Subjects concerned;

(ii) full details of the UO Personal Data compromised, including the categories and approximate number of UO Personal Data records concerned;

(iii) where known, details of the likely consequences of the Security Incident;

(iv) full details of how the Security Incident is being investigated and mitigation and remedial steps already put in place and to be put in place;

(v) contact details of personnel responsible for handling the Security Incident (if different from the contact details set out in clause 11.9);

(vi) individual measures which individual Data Subjects may adopt (if any) to mitigate harm that may be caused by the Security Incident; and

(vii) whether any Regulator, the Data Subjects themselves and/or the media have been informed or is otherwise already aware of the Security Incident, and their response.

(c) provide all such other cooperation and information reasonably requested by UO on an ongoing basis to assist in the investigation, mitigation and remediation of a Security Incident, including providing regular updates to UO in respect of the Security Incident and the matters described in clause 8(b); and

(d) unless expressly required under applicable laws, not communicate details of a Security Incident to any Regulator, Data Subjects and/or the media without UO's prior consent.

9. **Restricted Transfer**

(a) The Supplier shall not undertake a Restricted Transfer without UO's prior written consent. If UO provides consent in respect of a Restricted Transfer, the Parties agree to implement the relevant standard contractual clauses or other applicable data transfer mechanisms as permitted under Applicable Privacy Laws.

(b) Without limiting paragraph (a), the Supplier acknowledges and agrees that any Restricted Transfers made pursuant to the Agreement and this Addendum (including to Subprocessors) shall be made in compliance with Applicable Privacy Laws. Prior to making any Restricted Transfer, the Supplier 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 Supplier acknowledges that, in the event it transfers UO Personal Data pursuant to the Agreement and this Addendum (including to Subprocessors), it will undertake any corresponding data transfer impact assessment or a third party privacy or security impact 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 UO Personal Data and as otherwise required under Applicable Privacy Laws.

(d) Clauses 9(a) to (d) will not apply if the Supplier or the relevant Subprocessor is required to make a Restricted Transfer to comply with applicable law to which it is subject, in which case the Supplier will notify UO of such legal requirement prior to such Restricted Transfer unless such law prohibits notice to UO. The Supplier acknowledges and agrees that UO may object to the Supplier (or the Subprocessor) making such Restricted Transfer, to the extent such Restricted Transfer may expose UO to breach of Applicable Privacy Laws.

10. **Cooperation with Regulators and conduct of claims**

(a) The Supplier must promptly notify UO of all enquiries from a Regulator that the Supplier receives which relate to the Processing of UO Personal Data, the provision of the Products and/or Services, or either Party's obligations under this Addendum, unless prohibited from doing so under applicable law or by a Regulator. The Supplier shall (and shall procure each Subprocessor) not to disclose or make available to any Regulator any such UO Personal Data stored by the Supplier (or the Subprocessor, as appropriate) in the Chinese Mainland, except upon UO's written instructions or as required under applicable law.

(b) Subject to clause 10(d), the Supplier acknowledges that UO will handle all communications and correspondence with a Regulator relating to UO Personal Data and the provision of the Products and/or Services.

(c) UO will have the sole discretion to assume control of the defence and settlement of any third-party claims that relate to the Processing of UO Personal Data, including claims against the Supplier, its personnel or its Subprocessors, provided that UO will not enter into any settlement of such claim or compromise without the Supplier's prior written consent if such settlement or compromise would assert any loss or liability against the Supplier, increase the loss or liability (including under an indemnity) of the Supplier, or impose any obligations or restrictions on the Supplier (such as imposing an injunction or other equitable relief upon the Supplier). Where required, such consent shall not be unreasonably withheld or delayed. UO's exercise of such right will:

  (i) not be construed to require UO to bear the costs of such defence and settlement; and

  (ii) be without prejudice to UO's contractual, legal, equitable or other rights to seek recovery of such costs from the Supplier.

(d) The Supplier will be responsible for handling a particular communication or correspondence with a Regulator if:

  (i) UO notifies the Supplier that the Supplier will be responsible for such communication or correspondence; or

  (ii) a Regulator requests in writing to engage directly with the Supplier.

(e) Where the Supplier interacts directly with a Regulator in accordance with clause 10(d), the Supplier must at its own expense, consult and cooperate with UO throughout the entire interaction process. Any interactions with a Regulator will require the Supplier, its personnel and any Subprocessor to:

  (i) subject to clause 10(e)(iv), cooperate with, and make itself readily available for meetings with, the Regulator as reasonably requested;

(ii) answer the Regulator's questions truthfully and promptly;

(iii) subject to clause 10(e)(iv), provide the Regulator with such information and cooperation as the Regulator may require; and

(iv) unless prohibited by law, notify UO of any Regulator's request for information relating to UO Personal Data and before disclosing such requested information, the Supplier must fully cooperate with UO to prevent the disclosure of, or obtain protective treatment for such information, and comply with UO's instructions regarding the response to such a request.

11. General

11.1 Deletion or return of UO Personal Data

(a) Subject to clause 11.1(b), on expiry or termination of the Agreement, or upon request from UO at any time, the Supplier must immediately cease Processing any UO Personal Data and return to UO, or securely delete (at UO's direction), any UO Personal Data (including back-up copies) in the Supplier's possession or control.

(b) The Supplier may retain UO Personal Data only to the extent and for such period as required by applicable laws, provided that the Supplier notifies UO of the retention and at all times ensures the confidentiality of such UO Personal Data and ensures that any retained UO Personal Data is only Processed as necessary for the purposes specified in such laws requiring its retention and for no other purpose.

11.2 Indemnity

Notwithstanding any limitation or exclusion of liability set out in the Agreement, the Supplier must, at all times during and after the term of the Agreement, indemnify UO against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by UO arising out of or in connection with:

(a) any breach of Supplier's obligations under this Addendum;

(b) the Supplier's negligence or wilful misconduct in relation to any Processing of Personal Data; or

(c) any Security Incident.

11.3 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.

11.4 Exclusion of third-party rights

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

11.5 Governing Law

Except to the extent required by the applicable Standard Contractual Clauses, this Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

11.6 Order of precedence

The Supplier'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.

11.7 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 11.7(a), the Parties shall discuss the change in Applicable Privacy Laws and the Supplier will enter into and execute any additional appropriate documentation and safeguards as a result of any update of or changes to Applicable Privacy Laws as requested by UO.

11.8 Counterparts

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

11.9 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 UO Personal Data for the Party to the following addresses:

For UO:	For the Supplier:
Contact name: Data Protection Officer	Contact name: As listed in the Agreement
E-mail: DPO@hkexpress.com	E-mail: As listed in the Agreement

11.10 Structure of Addendum, definitions and interpretation

(a) This Addendum consists of:

(i) the main body of this Addendum, being clauses 2 to 12;

(ii) Annex A (Personal Data Processing Details); and

(iii) Annex B (Personal Data Security Measures).

(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; and

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

(c) In this Addendum:

Affiliate 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, and the PDPO, and any other applicable principles, industry codes and policies which may be applicable to the Processing of UO 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.

UO Personal Data means any Personal Data Processed by a Contracted Processor on behalf of UO pursuant to or in connection with the Agreement, as more particularly described in Annex A.

Contracted Processor means the Supplier or a Subprocessor.

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 means the European Union.

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 Supplier 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.

Products means the products provided by the Supplier to UO under the Agreement.

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 provision of the Products and/or Services; (b) the Processing of UO Personal Data in connection with the Products and/or Services; or (c) the Supplier's business or personnel relating to the Products and/or Services.

Restricted Transfer means (a) a transfer of UO 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 UO Personal Data from a Third Country.

Security Incident is defined in clause 8(a).

Services mean the services provided by the Supplier to UO under the Agreement.

Subprocessor means any third party (including the Supplier's Affiliate or the Supplier's subcontractor, but excluding any of their employees or Supplier's employees) appointed by or on behalf of the Supplier to Process UO Personal Data on behalf of UO pursuant to or in connection with the Agreement.

Subprocessor List is defined in clause 5(c). **Supplier** means the Party so identified at the start of this Addendum.

Standard Contractual Clauses means the standard contractual clauses formulated by countries or regions such as Europe, the United Kingdom, the United States, and China in accordance with Applicable Privacy Laws, aimed at ensuring the lawful, secure, and appropriate handling of data when personal information is transferred from one country to another. By signing the applicable standard contractual clauses, the protection of personal information is ensured to reach the same level as that of the applicable country. These standard contractual clauses typically include the obligations, responsibilities, and protective measures of both parties to ensure that data privacy and security are properly protected and comply with the relevant laws and regulations of the data exporting country.

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

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

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**", **"Personal Data"**, **"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.

12. **Legal Effect**

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

ANNEX A

This Annex A includes certain details of the Processing of UO Personal Data.

Item No.	Data requirement	Details of the Processing of UO Personal Data
1	**Subject matter and duration of the Processing of UO Personal Data**	The subject matter and duration of the Processing of UO Personal Data are set out in the Agreement and this Addendum.
2	**The nature and purpose of the Processing of UO Personal Data**	The nature and purpose of processing is for the performance of the Agreement.
3	**The types of UO Personal Data to be Processed**	Both UO and Supplier 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; (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 UO Personal Data to be Processed**	As listed in the Agreement, if any.

Item No.	Data requirement	Details of the Processing of UO Personal Data
5	**The categories of Data Subject to whom UO Personal Data relates**	Both UO and Supplier 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) 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.
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**	Not applicable unless otherwise agreed in the Agreement.
9	**Expected volume of Personal Data transferred**	As listed in the Agreement, if applicable.

ANNEX B – PERSONAL DATA SECURITY MEASURES

1. The Supplier 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 v1.1/2.0; and/or

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

(c) to the extent the Supplier 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 Annex 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 supplier engaged in the same or a similar type of business as that of the Supplier (within the aviation sector or otherwise) under similar circumstances.