Schedule XX

SITA SUPPLIER DATA PROCESSING AGREEMENT

Version: February 2024

This Data Processing Agreement (“DPA”) applies to [the Agreement to which it is attached as a schedule] /// [the agreement called _____ between SITA and_____ dated _____.] [EDIT AS NEEDED]

DEFINITIONS

The following definitions and interpretation apply in this “DPA:

The terms **"personal data", "controller", "processor", "processing", "data subject",** shall be interpreted in accordance with the definitions in Data Protection Legislation, and the term "process" shall be construed accordingly.

“**Affiliate”** has the meaning ascribed to it in the Agreement and, if not defined in the Agreement, means with respect to any person, any entity that directly or indirectly through one or more intermediaries Controls or is Controlled by such person or is under direct or indirect common Control with such person. “Control” means, in respect of an entity, the ability (whether it is legally enforceable or not) to control, whether directly or indirectly, the composition of the board of directors (or other governing body) of that entity, the voting rights of the majority of voting securities of the entity, or the management of the affairs of that entity.

"Agreement" means the agreement to which this DPA is incorporated into on the later of the date of execution of the Agreement or 26th May 2018.

"**Data Protection Legislation**" means all applicable data protection laws, regulations and mandatory codes of practice that apply to the Processing of personal data under this DPA and the Agreement.

"Restricted Transfer" means:

1. a transfer of SITA Data from SITA to SUPPLIER; and

2. any onward transfer of SITA Data from SUPPLIER to SUPPLIER’s Sub-processor (including any SUPPLIER Affiliate), or between two establishments of SUPPLIER.

in each case, where such transfer would be prohibited by Data Protection Legislation (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Legislation) in the absence of the Standard Contractual Clauses to be established under clause 4.3. or clause 5.3. below.

“Sensitive Data” has the same meaning as “special categories of data” in Data Protection Legislation.

"Services" means the services and any products provided by SUPPLIER to SITA pursuant to the Agreement.

"SITA" means the relevant subsidiary within the SITA group of companies which is a party to the Agreement to which this DPA is incorporated, and its Affiliates receiving Services from SUPPLIER.

"**SITA Data**" means all data (including personal data) in whatever form or medium which is (i) supplied, or in respect of which access is granted to SUPPLIER (or any approved third party) whether by SITA or otherwise in connection with the Agreement, or (ii) produced or generated by or on behalf of SUPPLIER (or any approved third party) in connection with the Agreement.

"Standard Contractual Clauses" means the approved standard EU contractual clauses described in Part B of this DPA.

"Sub-processor" means a processor other than SITA engaged by SITA to process SITA Data in connection with the Services (such as SUPPLIER) or engaged by SUPPLIER to process SITA Data in connection with the Services (such as third parties or SUPPLIER Affiliates).

"Supervisory Authority" means any competent data protection or privacy authority in any jurisdiction in which SITA is established, SUPPLIER provides the Services and/or in which SUPPLIER processes personal data.

"SUPPLIER" means the party providing the Services to SITA under the Agreement to which this DPA is attached, and any of its Affiliates.

Terms and expressions used in this DPA and not defined herein have the meanings assigned to them in the Agreement to which this DPA is incorporated.

NOT WITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, IN THE EVENT OF ANY CONFLICT OR INCONSISTENCY BETWEEN THE TERMS OF THE AGREEMENT (OTHER THAN THIS DPA) AND THE TERMS OF THIS DPA, THE TERMS OF THIS DPA WILL PREVAIL.

PART A – DATA PROCESSING

1. Roles and Responsibilities

1.1 SUPPLIER and SITA agree that for the purposes of this DPA and SUPPLIER's processing of the SITA Data in connection with the Services to be provided, SUPPLIER (and each permitted Sub-processor pursuant to this DPA) shall be a processor and/or Sub-processor.

1.2 The SUPPIER will comply with Applicable Data Protection Legislation when processing SITA Data under this Agreement.

2. Details of Processing

2.1 The subject-matter of processing of SITA Data by the SUPPLIER is the performance of the Services pursuant to the Agreement. The duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects processed under this DPA are further specified in PART A to this DPA.

2.2 The Parties agree the following terms shall apply to processing of all SITA Data regardless of its origin or the applicable law:

Subject matter of processing	_____ [SUPPLIER to insert subject matter (eg. description of the Services)]
Duration of processing	_____ [SUPPLIER to insert duration (eg. length of contract)]
Nature of processing	_____ [SUPPLIER to insert nature of processing (eg. components of the Services or refer to service scope)]
Purpose of processing	_____ [SUPPLIER to insert purpose / nature of Services)]
Type of personal data	_____ [SUPPLIER to insert the types of personal data being processed (e.g. name, date of birth, address, passport no, phone, email, etc.) or refer to service scope Schedule or Appendix].
Categories of data subjects	[SUPPLIER to list the categories of data subjects]

3. Processor Obligations

Where SUPPLIER processes SITA Data on behalf of SITA, SUPPLIER shall:

3.1 only process the SITA Data in compliance with, and shall not cause itself or SITA to be in breach of, Data Protection Legislation.

3.2 only process the SITA Data on the documented instructions of SITA as specified in the Agreement, this DPA or as otherwise communicated by SITA to perform its obligations under this Agreement and not for any other purposes, including retaining, using, disclosing, or selling the personal data for a commercial purpose other than providing the Services specified by SITA's documented instructions. If any other processing is required by applicable Data Protection Legislation, SUPPLIER shall inform SITA of the legal requirement before commencing such processing, unless providing this information to SITA is legally prohibited;

3.3 notify SITA without delay if SUPPLIER is of the opinion that an instruction of SITA is not in compliance with Data Protection Legislation;

3.4 inform SITA without undue delay of any enquiry, complaint, notice or other communication it receives from any Supervisory Authority or any individual, relating to either SUPPLIER's or third parties' appointed by SUPPLIER in connection with the Services or SITA's compliance with Data Protection Legislation. SUPPLIER shall provide all necessary assistance to SITA to enable SITA to respond to such enquiries, complaints, notices or other communications and to comply with Data Protection Legislation. For the avoidance of doubt, SUPPLIER shall not respond to any such enquiry, complaint, notice or other communication without the prior written consent of SITA;

3.5 on termination or expiry of the Agreement, for whatever reason, cease all use of the SITA Data and shall, at SITA's election, either destroy all SITA Data or transfer all SITA Data to SITA or a nominated third party in a mutually agreed format and by a mutually agreed method and confirmed in writing. A data destruction certificate is to be provided if appropriate;

3.6 take all reasonable steps to ensure any staff who may have access to SITA Data are subject to appropriate obligations of confidentiality and at all times act in compliance with Data Protection Legislation and the obligations of this DPA;

3.7 implement all appropriate technical and organizational measures to ensure security of the SITA Data including protection against unauthorized or unlawful processing (including without limitation unauthorized or unlawful disclosure of, access to and/or alteration of SITA Data) and against accidental loss, destruction or damage.

That shall include:

a) ensuring any staff who may have access to SITA Data are subject to appropriate obligations of confidentiality and at all times act in compliance with Data Protection Legislation and the obligations of this DPA;

b) comply with security requirements as described in Part C, as reasonably updated and notified to SUPPLIER from time to time;

c) Any processing of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

(i) training of personnel;

(ii) encryption of data in transit and at rest;

(iii) system access logging and general data access logging.

3.8 provide SITA with co-operation and assistance in performing data protection impact assessments, security of processing and complying with any data subject rights (including access requests) received by, or on behalf of, SITA;

3.9 subject to, and save where authorized to transfer to its Sub-processors as set forth in clause 5, not transfer and/or disclose any SITA Data to any other party without the prior specific written consent of SITA and unless permitted by Data Protection Legislation and is able to demonstrate a legal basis for the transfer;

3.10 save where SUPPLIER has in respect of a particular Sub-processor complied with the requirement to enter into the Standard Contractual Clauses with the Sub-processor as set forth in clause 5 not transfer any SITA Data outside the European Economic Area (EEA), UK or Switzerland or to any international organizations without the express prior written consent of SITA;

3.11 permit SITA, or a third-party auditor acting under SITA's direction, to conduct no less than once a year, or in the event of a data breach involving SITA Data, and at SITA's cost, unless the audit arises in relation to a data breach involving SITA Data, data privacy and security audits, assessments and inspections concerning SUPPLIER's data security and privacy procedures relating to the processing of SITA Data, its compliance with this DPA and Data Protection Legislation. SITA may, in its sole discretion, require SUPPLIER to make available all information necessary to demonstrate SUPPLIER's compliance with this DPA and these procedures in lieu of conducting such an audit, assessment or inspection;

3.12 notify SITA in writing by sending an e-mail at this address SIRT@sita.aero without undue delay, but no later than 36 hours after it becomes aware of any reasonably suspected or confirmed unauthorised or unlawful processing, disclosure of, or access to, SITA Data and/or any accidental or unlawful destruction of, loss of, alteration to, or corruption of SITA Data (a Data Breach) and provide SITA, as soon as possible, with complete information relating to a Data Breach, including, without limitation:

a) the nature of the Data Breach and estimated duration of the breach;
b) the nature of the personal data affected, the categories and number of data subjects concerned, the number of personal data records concerned;
c) measures taken or proposed by SUPPLIER to address the Data Breach and the possible adverse effect of the Data Breach;

d) SUPPLIER shall maintain a log of Data Breaches including facts, effects, investigative steps, conclusions and remedial action taken;
e) where it is possible to do so, SUPPLIER shall take all steps to restore, re-constitute and/or reconstruct any SITA Data which is lost, damaged, destroyed, altered or corrupted as a result of a Data Breach as if they were SUPPLIER's own data at its own cost with all possible speed and shall provide SITA with all reasonable assistance in respect of any such Data Breach; and
f) not release or publish any filing, communication, notice, press release, or regulatory report concerning the Data Breach without SITA's prior written approval (except where required to do so by law)., SUPPLIER will provide reasonable notice to SITA of such a requirement).

3.13 SITA reserves the right to specify the selected hosting region(s) for the Hosted Services ("Region"). Once SITA has selected a Region, SUPPLIER will not store SITA Data or SITA Data outside the Region.

3.14 SITA's selection of region is: the European Union. [EDIT IF AGREED AND APPROVED BY LEGAL/PRIVACY]

4. Data Transfers

4.1 SUPPLIER shall only receive and/or process SITA Data at the locations agreed upon in the Agreement or this DPA and shall not transfer personal data across country borders unless expressly authorized in writing by SITA and in compliance with such legally enforceable mechanism(s) for transfers of SITA Data as may be permitted under Data Protection Legislation from time to time.

4.2 In the event that SUPPLIER receives or processes any SITA Data transferred from the European Union, the European Economic Area and/or its member states, Switzerland and/or the United Kingdom to countries that do not ensure an adequate level of data protection within the meaning of the Data Protection Legislation and Regulations of the foregoing territories, Section 1.4 (c) and Part C of this DPA shall apply.

4.3 SITA (as "data exporter") and SUPPLIER (as "data importer") hereby enter into either the: (1) Standard Contractual Clauses (Module 2: Controller to Processor) where SITA is a controller; or (2) Standard Contractual Clauses (Module 3: Processor to Processor) where SITA is a processor; and addendum in the case of transfers out of the UK in the manner described in Part B in respect of any Restricted Transfers:

a) from SITA to SUPPLIER; and/or
b) where both SITA and SUPPLIER are outside of both the EEA and a third country subject to an adequacy decision under the GDPR, and SUPPLIER processes personal data, received by onward transfer from SITA, originating from any data subjects that are EEA-resident (e.g. EEA-resident passengers, customers, employees and contractors).

4.4 In addition, SITA (as "data exporter") and SUPPLIER (as "data importer") hereby agree that any data transfer based on an approved transfer mechanism will be complemented by an assessment. SUPPLIER shall assist SITA in providing information relevant for such transfer assessment under Data Protection Legislation.

5. Sub-processors.

5.1 SITA authorizes SUPPLIER to appoint or sub-contract Sub-processors in accordance with this section 5 and any restrictions in this DPA:

a) subject to and save where authorized to transfer to its Sub-processors as set forth in clause 5.1., not transfer and/or disclose any SITA Data to any other party without the prior specific written consent of SITA and unless permitted by Data Protection Legislation and is able to demonstrate a legal basis for the transfer;
b) save where SUPPLIER has in respect of a particular Sub-processor complied with the requirement to enter into the Standard Contractual Clauses with the Sub-processor as set forth in clause 5.3.(c) and with clauses 5.3.(a) and (b), not transfer any SITA Data outside the European Economic Area (EEA), UK or Switzerland to any international organizations without the express prior written consent of SITA.

5.2 SUPPLIER may continue to use those Sub-processors already engaged by SUPPLIER as at the date of entry into this DPA, subject to SUPPLIER in each case as soon as practicable meeting the obligations set out in clause 5.3.:
a) SUPPLIER shall give SITA 60 days prior written notice by sending an e-mail at this address: Supplier.Security@sita.aero cc Supplier.Security@sita.aero of the appointment of any new Sub-processor, including full details of the processing to be undertaken by the Sub-processor. If within 30 days of receipt of that notice, SITA notifies SUPPLIER in writing of any objections (on reasonable grounds) to the proposed appointment;
b) SUPPLIER shall work with SITA in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor (including but not limited to appointing an alternative Sub-processor satisfactory to SITA); and
c) Where such a change cannot be made within 60 days from SUPPLIER's receipt of SITA's notice, notwithstanding anything in the Agreement, SITA may by written notice to SUPPLIER with immediate effect terminate the Services which require the use of the proposed Sub-processor, with no further liability to SITA other than to pay fees for the Services up to date of termination (and SITA shall be refunded for any advance payment of fees for Services following the date of termination).

5.3 With respect to each Sub-processor, SUPPLIER shall:
a) Before the Sub-processor first processes SITA Data (or, where relevant, in accordance with clause 5.2., carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for SITA Data required by this DPA;
b) enter into a written agreement with all Sub-processors containing obligations on such Sub-processors which are no less onerous than those set out in this DPA;
c) enter into: Standard Contractual Clauses (and addendum in the case of transfers out of the UK) with all Sub-processors: (1) where there is any Restricted Transfer between SUPPLIER and the Sub-processor; and/or (2) where SUPPLIER and its Sub-processor are both outside of both the EEA and a third country subject to an adequacy decision under the GDPR, and Sub-Processor processes personal data, received by onward transfer from SUPPLIER, originating from any data subjects specified in clause 2.2 that are EEA-resident (e.g. EEA-resident passengers, customers, employees or contractors); and

d) provide to SITA for review such copies of its above agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Annexure) as SITA may request from time to time.

5.4 The list of Sub-Processors used to provide the Services and their country or location of processing may be requested at any time by SITA. A copy of this list, current as of Effective Date, set forth in Annex I to this DPA.

6. SUPPLIER will provide SITA with such assistance and co-operation as SITA may reasonably request to enable SITA to comply with any of its obligations under Data Protection Legislation, including but not limited to obligations in connection with data subject rights and data processing impact assessments.

7. SUPPLIER shall, immediately on demand, fully indemnify SITA and keep SITA fully and effectively indemnified against all costs, claims, demands, expenses (including legal costs and disbursements on a full indemnity basis), losses (including indirect losses and loss of profits), actions, proceedings and liabilities of whatsoever nature arising from or incurred by SITA in connection with any failure of SUPPLIER or any third party appointed by SUPPLIER to comply with the provisions of this Clause 1, and Standard Contractual Clauses entered into between the parties, and/or Data Protection Legislation in respect of its processing of SITA Data. The parties agree that the indemnity in this clause is limited by the monetary cap on liability contained in the Agreement. The parties agree that the liability cap will not apply in the following cases: (i) SUPPLIER does not follow SITA's instructions for processing; (ii) SUPPLIER does not follow its security and technical and organizational measures ((TOMs); and (iii) SUPPLIER performs an unauthorized data transfer.

8. SUPPLIER is obligated to provide all reasonable assistance to SITA, including but not limited to any reasonable requests to amend this DPA, or the Standard Contractual Clauses (and addendum in the case of transfers out of the UK) between the parties, based on changes in Data Protection Legislation.

ANNEX I

LIST OF SUB-PROCESSORS [To be filled-in by SUPPLIER]

As of the Effective Date, the following is a list of sub-processors engaged in the provision of the products/services:

Number	Products/ Services	Subprocessor Name	Physical Address/Location	Type of Products/Services Provided

PART B – STANDARD CONTRACTUAL CLAUSES & THIRD COUNTRY PROCESSING AGREEMENTS

ADDENDUM A

EUROPEAN ECONOMIC AREA ADDENDUM

1. Definitions

1.1 "EEA" means the European Economic Area.

1.2 "European Data Protection Law" means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" or "GDPR"), as implemented by countries within the EEA and/or other laws that are similar, equivalent to, or successors to the GDPR.

1.3 "Model Clauses" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses (SCCs) for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.4 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law. All references to Data Protection Legislation or laws in the DPA shall be read in the context of EU or Member State Law for the purpose of this Addendum.

2. International Transfers

2.1 To the extent that SUPPLIER processes any personal data from the EEA and transfers such personal data outside of the EEA to countries not deemed "adequate" by the European Commission, the Parties agree to enter into and comply with the Standard Contractual Clauses (SCCs) described in Section 3 of this Addendum.

3. Standard Contractual Clauses (SCCs)

3.1 The Model Clauses, as set out at this link, apply to this DPA, and the parties agree that the signing of this DPA constitutes deemed signature and incorporation of those standard contractual clauses (and the appendices to same) as required:

a) **For Module 2 (Controller to Processor) transfers: https://www.sita.aero/gdpr/scc/suppliers/module2**
b) **For Module 3 (Processor to Processor) transfers: https://www.sita.aero/gdpr/scc/suppliers/module3**

3.2 In respect to Clause 9(a) Sub-processors of Module Two of the Model Clauses, SITA grants SUPPLIER a General Written Authorization for the use of Sub-processors listed here: Annex 1 to this DPA

3.3 In respect to Clause 17 Governing Law: In each case of data exporting, the law of the Member State from which SITA or its Affiliate is exporting data.
3.4 In respect to Clause 18 Choice of forum and jurisdiction: in each case of data exporting, the law of the Member State from which SITA or its Affiliate is exporting data.

ANNEX I TO ADDENDUM A

A. List of Parties

Data exporter: The data exporter is the entity identified as the Customer in the Agreement, acting as a data exporter on behalf of itself and its Affiliates.

Data importer: The data importer is SITA, acting as a data importer on behalf of itself and its Affiliates.

B. Description of Transfer

1. Categories of Data Subjects whose personal data is transferred: The personal data transferred may relate to the following categories of data subjects: Passengers of the Customer and/or staff of the and/or other individuals whose personal data is processed as part of the provision of the services/products.
2. Types of personal data transferred: The personal data transferred may relate to Passenger personal data to enable air transport – being:
   a. names, email addresses, dates of birth, genders, addresses, passport numbers; and
   b. customer staff data – being names, email addresses,

in accordance with the requirements set out in Service description.

3. Sensitive data transferred (if applicable): When processing personal data, SUPPLIER may process sensitive personal data. The nature and scope of the sensitive personal data that is transferred may not be known until after the processing has taken place and may include: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
4. The frequency of the transfer (e.g., Whether the data is transferred on a one-off or continuous basis): The transfer of personal data between the Parties will occur on a continuous basis.
5. Nature of the Processing: personal data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analysing, collecting, transferring, and making available personal data.
6. Purpose: The purpose of the processing of personal data under this DPA is to enable SUPPLIER to deliver the services/products and perform its obligations as set forth in the Agreement (including this DPA) mainly related to communications and/or air transport services as per the Service description or as otherwise agreed by the Parties in mutually executed written form. See description of Service in Service Agreement.
7. The period for which the personal data will be retained, or if that's not possible, the criteria used to determine that period: SUPPLIER will retain personal data to fulfil the purposes for which it was collected – either as authorized by SITA or following mandatory legal provisions and as necessary to comply with business requirements, legal obligations, resolve disputes, and enforce its rights. Specific data retention periods are reflected for certain Products here.

8. For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing: personal data may be transferred to SUPPLIER Sub-processors.

C. Competent Supervisory Authority

Competent supervisory authority/ies to be chosen in accordance with Clause 13.

ANNEX II TO ADDENDUM A

Description of the technical and organizational measures implemented by the data importer(s)

SUPPLIER Technical and organization security measures (TOMs) can be found at: [Attachment A] [SITA | SITA suppliers] [insert link to SUPPLIER TOMs or put them as an attachment]

ADDENDUM B

SWITZERLAND ADDENDUM

1. Terms

All terms used herein not defined in the DPA will have the meaning assigned to them in the FADP. All references to Data Protection Legislation, Law or Laws in the DPA shall be read in the context of FAPD for the purpose of this Addendum.

2. International Transfers

To the extent that SUPPLIER processes any personal data from Switzerland and transfers such personal data outside of Switzerland to countries not deemed to provide an adequate level of data protection under FADP, the Parties agree to enter into and comply with the Standard Contractual Clauses (SCCs) as defined and included in the European Economic Area Addendum to this DPA and further amended by this Addendum. SUPPLIER agrees that it is a "data importer" and SITA is the "data exporter" under the SCCs (as amended by this Addendum).

3. Model Clauses. For the purposes of this Addendum:

3.1 Module Two (Controller to Processor) (and/or Module Three (Processor to Processor) of the SCCs set forth in the European Economic Area Addendum to this DPA, including all of its Annexes, is incorporated by reference into this Addendum. Signatures applied to the Agreement will be taken as equally signing and effectuating the SCCs.

3.2 All references to the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“General Data Protection Regulation” and/ or “GDPR”) shall be deemed to refer to the FADP.

3.3 All references to the competent supervisory authority shall be deemed to refer to the Federal Data Protection and Information Commissioner (“FDPIC”).

3.4 All references to Member State(s)/EU Member State(s) shall be deemed to include Switzerland.

3.5 All references to the exporter in the EU shall be deemed to include the exporter in Switzerland.

3.6 All reference to Clause 8.8 of Module Two and in Annex I to the EEA shall be deemed to include Switzerland.

3.7 Where the SCCs use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP.

ADDENDUM C

UNITED KINGDOM ADDENDUM

1. Definitions

1.1 "Mandatory Clauses" means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s19A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

1.2 "Model Clauses" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.3 "UK" means the United Kingdom.

1.4 "UK Data Protection Law" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including: (i) the UK GDPR and UK Data Protection Act 2018; and/or (ii) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) above.

1.5 "UK GDPR" as defined in section 3 of the Data Protection Act 2018.

1.6 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law. All references to Data Protection Law or laws in the DPA shall be read in the context of UK Law for the purpose of this Addendum.

2. International Transfers

2.1 To the extent that SUPPLIER processes any personal data from the UK and transfers such personal data outside of the UK to countries not deemed to provide an adequate level of data protection under UK Data Protection Law, the Parties agree to enter into and comply with the Model Clauses (as amended by the Mandatory Clauses). SUPPLIER agrees that it is a "data importer" and SITA is the "data exporter" under the Model Clauses (as amended by the Mandatory Clauses).

2.2 The Parties agree that the data export solution identified in Section 3 (Mandatory Clauses) will not apply if and to the extent that SUPPLIER adopts an available, alternative data export solution for the lawful transfer of personal data (as recognized under UK Data Protection Law) outside of the UK. To the extent the execution of additional documents is required to give effect to such data export solution, the Parties will work in good faith to execute such documentation.

3. Mandatory Clauses

3.1 The Mandatory Clauses, as set out at this link https://www.sita.aero/gdpr/scc/UKaddendum , apply to this DPA and the parties agree that the signing of this DPA constitutes deemed signature and incorporation of those mandatory clauses (and the appendices to same). The Mandatory clauses are incorporated by reference into this Addendum and the Model Clauses are amended in accordance with the Mandatory Clauses. For clarity, Annexes I and II of the Model Clauses included in the European Economic Addendum (Addendum A to this DPA) are incorporated by reference to this Addendum.

3.2 Neither the Mandatory Clauses or this Addendum shall be interpreted in a way that conflicts with rights and obligations provided for under UK Data Protection Law.

3.3 SUPPLIER (as data importer) may end this DPA (including this Addendum) to the extent the Mandatory Clauses apply, in accordance with Section 19 of the Mandatory Clauses.

3.4 For the purposes of this Addendum: the competent supervisory authority shall be the Information Commissioner's Office.

3.5 For the purposes of this Addendum, clause 3.1 to 3.2.1 of the European Economic Area Addendum are incorporated and shall be read and interpreted in accordance with the Mandatory Clauses.

3.6 In respect to Clause 17 Governing Law: The governing law is that of England and Wales.

3.7 In respect to Clause 18 Choice of forum and jurisdiction: The courts of England Wales shall resolve any disputes arising from the Model Clauses (as amended by the Mandatory Clauses).

ADDENDUM D

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

All terms used herein not defined in the DPA or this Addendum, will have the meaning assigned to them in the CCPA and its implementing regulations.

SUPPLIER will comply with the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act (together, the “CPRA”) as a “service provider” (as defined by the CPRA) in its performance of the Products.

SUPPLIER shall not:

1. Sell Personal Information.
2. Retain, use, or disclose Personal Information outside of the direct business relationship between

SUPPLIER and SITA or for any purpose other than for the business purposes specified in the Agreement (including the DPA) or as otherwise permitted by the CPRA.

PART C – SUPPLIER SECURITY

1. General Security Provisions

1.1 SUPPLIER shall comply with either 1.1(a) or 1.1(b) below:

a. SUPPLIER shall maintain and comply with the following certifications during the term of this Agreement, that cover the Services and their associated systems, networks, applications, and underlying components, and shall at all times during the term of this Agreement maintain and perform the technical and organisational security measures included in such certifications:

ISO/IEC 27001 certification;
ISAE3402 SOC2 Type II report; or SOC 3 Type II report
PCI DSS compliance (where credit card data is handled);

SUPPLIER shall provide evidence of such certifications and documentation to SITA no less than once per calendar year. The standards specified in this clause shall be replaced by future equivalent standards if/when such standards are superseded.

b. If SUPPLIER does not maintain and comply with the certifications required by clause 1.1(a) above, SUPPLIER shall during the term of this Agreement comply with the detailed security requirements in clause 2.1 below in respect of the Services and their associated systems, networks, applications, and underlying components.

1.2 SUPPLIER shall plan and maintain disaster recovery and business continuity management programs to counteract interruptions and protect critical business processes from the effects of major failures and disasters. These programs must be tested at least annually and comply with ISO 20000, 27002, and 15408.

1.3 SUPPLIER shall comply with all applicable data privacy legislation in respect of the Services.

1.4 SUPPLIER agrees and warrants to SITA that the Services and/or products and/or deliverables and/or supporting systems (as appropriate) supplied by the SUPPLIER to SITA under this Agreement are appropriate to the risk, using all applicable preventative, detective and corrective measures, administrative, physical and technical controls, to ensure SITA Data and information systems are appropriately protected from unauthorized disclosure, alteration and unavailability

1.5 SUPPLIER shall report to SITA, within 36 hours of discovery, any known or suspected unauthorized access, use, misuse, disclosure, destruction, theft, vandalism, modification, or transfer of SITA proprietary information or data. Reports should be by sent via email to the SITA Security Incident Response Team (SIRT@SITA.aero). SUPPLIER will provide SITA with reasonably requested support and information about such security incident and status of any SUPPLIER remediation and restoration activities.

1.6 SUPPLIER will designate a Security Point of Contact within SUPPLIER's organization to act as the liaison between SITA and SUPPLIER.

1.7 SITA may audit compliance of SUPPLIER with Clauses 1.1 & 1.2 above once per calendar year not standing in the event of SUPPLIER informing SITA of a data incident where SITA will exercise its audit rights regardless of any audit having taken place that calendar year

1.8 Without prejudice to SITA's rights to audit SUPPLIER under this Part C, SUPPLIER shall provide to SITA reports and information demonstrating compliance with specific security measures set forth in this Part C, if and when requested by SITA, at no additional charge.

1.9 Except to the extent the liability arises as a result of the action or omission of SITA, SUPPLIER shall indemnify, protect and hold harmless SITA against any liability whatsoever incurred by SITA, including any reasonable costs, claims, demands and expenses arising out of or in connection with such liability (including reasonable legal costs), arising from any failure to perform, and/or failure to comply with the requirements of this Part C, and/or arising from any breach of Clauses 1.1 or 1.2.

1.10 SUPPLIER will maintain and follow documented incident response policies consistent with industry best practices and will comply with data breach notification terms of the Agreement. SUPPLIER will investigate unauthorized access and unauthorized use of SITA Data of which SUPPLIER becomes aware (security incident), and, within the Service scope, SUPPLIER will define and execute an appropriate response plan.

1.11 SUPPLIER will protect the SITA Data upon termination of the Agreement and will securely delete data when no longer required to prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for data deletion.

2. Detailed Security Requirements if SUPPLIER does not comply with the Certifications required by clause 1.1(a). If SUPPLIER does not maintain and comply with the certifications required in clause 1.1(a), it must instead maintain and comply with all the following requirements:

2.1 SUPPLIER will maintain and follow IT security policies and practices that are integral to SUPPLIER's business and mandatory for all SUPPLIER employees, including supplemental personnel.

2.2 SUPPLIER will review its IT security policies at least annually and amend such policies as SUPPLIER deems reasonable. SUPPLIER will notify SITA of any changes to the Provider's security policy.

2.3 SUPPLIER will maintain and follow its standard mandatory employment verification requirements for all new hires, including supplemental employees, and extend such requirements to wholly owned SUPPLIER subsidiaries. These requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by SUPPLIER.

2.4 SUPPLIER employees will undergo security and privacy training and awareness to ensure they comply with SUPPLIER 's security policies, and records of training should be maintained. For certain security tasks, the SUPPLIER must ensure their staff members are properly trained and certified (e.g., CISSP) and will provide evidence of being so upon reasonable request by SITA.

2.5 SUPPLIER will ensure that all employees and representatives who will perform work or have access to information resources associated with SITA are covered by binding/signed non-disclosure agreements.

2.6 SUPPLIER will ensure that physical SUPPLIER related work areas are secure to prevent unauthorized physical access, damage and interference. SUPPLIER will restrict and limit access to SITA Data and SITA information systems by defining roles and segregating duties (to avoid conflicts of interest in security activities), establishing authorization processes and by implementing a technical solution that manages the access rights of users from their onboarding to the end of their assignment and access rights. Access rights to SITA Data and information systems will be periodically reviewed.

2.7 Consistent with industry standard practices, and to the extent supported by each component managed by SUPPLIER within the Service, SUPPLIER will enforce timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, implement dual-factor authentication whenever possible, ensure accesses are uniquely identifying a person and/or a system and maintain sufficient audit records of accesses for at least thirty days. SUPPLIER will ensure that authentication mechanisms cannot be overcome.

2.8 SUPPLIER will limit the number of privileged users and will appropriately monitor their access with extensive logging.

2.9 SUPPLIER personnel remotely accessing Systems and data in relation to the Service will be individually identified and authenticated using two-factor authentication, and their login attempts will be monitored.

2.10 SUPPLIER will ensure that the termination process for its employees includes return of, and revoking of access rights to, all SITA information assets.

2.11 SUPPLIER shall maintain logs of all Events on systems and networks used to process personal data (“Event Logs”), including information such as date, time, user ID, device accessed, and port used. SUPPLIER shall maintain such Event Logs for a minimum period of twelve (12) months. If requested by SITA, SUPPLIER shall allow SITA to analyse the Event Logs for security related events, unusual activities and other issues, such as unsuccessful attempts to create backup copies of data. For the purpose of this section, “**Event**” shall mean: any incident that may result in damage to any information security assets, personal data, and/or operations of systems and networks.

2.12 SUPPLIER will secure all SITA Data by encrypting the data and/or the link between the two communication ends, using reliable implementations of network protocols and encryption algorithms, in compliance with legal requirements in the country of operation and as recommended by security best practices. SUPPLIER will communicate to SITA the secure network protocols and encryption algorithms used.

2.13 SUPPLIER will encrypt SITA stored sensitive data, including personal data, on all information systems deemed sensitive, using reliable encryption algorithms (compliant with FIPS 140-2) in compliance with legal requirements in the country of operation and as recommended by security best practices.

2.14 SUPPLIER will perform or have performed annual penetration testing on all deemed sensitive information systems or upon major service changes, while avoiding operational and business disruption.

2.15 SUPPLIER will implement antimalware solution and anti-phishing mechanisms on all relevant information systems.

2.16 SUPPLIER will subscribe to an external threat intelligence service in order to receive regular timely information of current threats and technical vulnerabilities for all relevant information systems. SUPPLIER will build a patch management process based on current best practice.

2.17 SUPPLIER will implement Next Generation firewalls with dedicated rulesets/policies that will be periodically reviewed as part as the general security review process. The technologies used will be regularly updated as part of the patch and vulnerability management process.

2.18 SUPPLIER will perform automatic vulnerability scanning, while avoiding operational and business disruption.

2.19 SUPPLIER will assess business impacts and security risks regarding all relevant information systems, at least annually and upon any major change in the operating environment.

2.20 SUPPLIER will implement an effective backup and restore strategy regarding SITA Data and implement reliable technology to support its strategy. Backed up data at rest should be encrypted within its container, data sent between the backup server and the backed-up resources should be encrypted in transit. At least one backup copy should be kept on a remote location, not subject to natural threats (e.g. flood).