# DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter, the "DPA") made effective as of the same data as the Service Agreement (the "***Effective Date***") supplements the "Service Agreement" with respect to the "Services" (both terms as defined below) performed by ARINC Incorporated (a part of Collins Aerospace) having its place of business at 2551 Riva Road, Annapolis MD 21401 USA and/or its Affiliates (collectively "***ARINC***") on behalf of your company and/or its Affiliates (collectively the "***Customer***").

**WHEREAS**, ARINC and Customer have entered into the "Service Agreement" under which ARINC, and/or other ARINC Affiliates, performs or will perform certain "Services" for or on behalf of Customer and/or other Customer Affiliates;

**WHEREAS**, in performing such Services, ARINC may be processing Personal Data as part of delivering the Services;

**WHEREAS**, it is therefore necessary for the Customer to ensure that ARINC's Processor obligations under applicable Data Protection Laws are in writing and binding upon ARINC.

**NOW, THEREFORE**, in its performance of the Services for the Customer, ARINC hereby agrees to be bound by the following terms and conditions with respect to its Processing of Personal Data:

## 1. DEFINITIONS

Capitalised terms shall have the meanings set out below. Any capitalised terms not defined below or defined elsewhere in this DPA shall have the meanings as ascribed in the Service Agreement:

1.1 **"Affiliate"** means in relation to a party, any entity which (directly or indirectly) controls, is controlled by and/or under common control with that party.

1.2 "**Controller**," "**Processor**," "**Subprocessor**," "**Data Subject**," and "**Data Exporter**" and shall have the same meaning as in the Data Protection Laws.

1.3 "**Data Protection Laws**" means, as and to the extent they apply, in relation to any Personal Data which is Processed in the performance of the Services Agreement, any applicable laws and regulations in relation to the privacy or Processing of Personal Data relating to identifiable individuals, the protection of personal information or data, and the cross-border transfer of personal information or data, including as may be applicable, but not limited to: (a) the California Consumer Privacy Act ("CCPA"); (b) the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"); and (c) national laws implementing, revising or replacing the GDPR, each as updated, amended or replaced from time to time.

1.4 "**Governmental Agencies**" means governmental and/or quasi-governmental agencies, airport authorities, passport agencies, customs officials, and such similar entities.

1.5 **"Personal Data"** means any information relating to an identified or identifiable data subject or as otherwise defined by applicable law;

1.6 **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

1.7 **"Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction and "Processed" or "Processing" shall be construed accordingly.

1.8 "**Pseudonymous Data**" means information processed in such a manner that Personal Information can no longer be attributed to a specific Data Subject.

1.9 "**Service Agreement**" means the service agreement executed by and between ARINC and the Customer for ARINC's delivery of the "Services" defined in Section 1.10 hereinbelow.

1.10 "**Services**" means ARINC's Processing of Personal Data on behalf of the Customer as related to ARINC's provision of the products and services set forth in the Service Agreement.

## 2. PROCESSOR OBLIGATIONS

2.1 Data Processor. With respect to the Services, ARINC is the Processor of Personal Data and Customer is the Controller of Personal Data.

2.2 Processing. ARINC shall Process the Personal Data to perform the Services and in accordance with Customer's documented instructions, which such instructions may be present in the Service Agreement. If the Services Agreement involves collection or Processing of Personal Data from individuals in California, ARINC is a "Service Provider", as such term is defined in the California Consumer Privacy Act, Cal, Civ. Code §§ 1798.100 et. seq. and implementing regulations (the "CCPA"), and will neither sell, nor exchange for anything of value, Personal Data.

2.3 Confidentiality. ARINC shall maintain the confidentiality of any such Personal Data and shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is limited to those individuals who need to access the relevant Personal Data, for the purposes necessary to perform the Services hereunder.

2.4 Technical and Organization Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, ARINC shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2.5 Subprocessors. ARINC may engage the services of Subprocessors to perform the Services, and in doing so: (i) will execute written agreements with its Subprocessors binding them to terms no less rigorous than those set forth herein; and (ii) agrees to be responsible for the Subprocessors obligations. ARINC's compliance with the foregoing requirement shall suffice as authorized approval of ARINC's selected Subprocessors. Upon request, ARINC shall make available to Customer a list of Subprocessors that ARINC subcontracts with in the Processing of Personal Data. In the event that the Customer sends notification to ARINC setting forth its reasons for disapproving any of the listed Subprocessors, ARINC agrees that the Customer thereby reserves the right to terminate the Services effective upon thirty (30) days to the extent that ARNC in unable or unwilling to substitute an alternate Subprocessor.

2.6 Data Subject Requests. ARINC shall notify Customer if ARINC receives a request from a Data Subject exercising his/her data subject rights under applicable Data Protection Laws and ARINC shall cooperate with Customer in responding to such request. ARINC shall not respond to any Data Subject request unless required by applicable law.

2.7 Notification of Data Breach. To the extent that ARINC experiences a Personal Data Breach with respect to the Personal Data ARINC Processes as part of its performance of the Services, ARINC will notify Customer promptly upon becoming aware of such Personal Data Breach, to the extent required under applicable law. ARINC will mitigate, to the extent practicable, any harmful effect of such Personal Data Breach.

2.8 Cooperation. ARINC will provide reasonable assistance to Customer with any its protection impact assessment and/or with any prior consultations to any supervisory authority, to the extent required by applicable law, in each case solely in relation to Processing of Personal Data by ARINC on behalf of Customer and as such Processing relates to the Services.

2.9 Destruction of Personal Data. Unless as otherwise instructed by the Customer or as required by applicable law, ARINC shall, after the end of the provision of Services, either (at the choice of Customer and as operationally feasible): (i) return a complete copy of all Personal Data to the Customer by secure file transfer and securely wipe all other copies of Personal Data Processed by ARINC or its Subprocessors; or (ii) securely wipe all copies of Personal Data Processed by ARINC or any of its Subprocessors.

2.10 Data Analytics. In connection with the provision of the Services hereunder, ARINC may use Pseudonymous Information for data analytics to improve the Services, which Customer hereby authorizes ARINC to use in accordance with carrying out its obligations under the Services Agreement. Subject to the ARINC's compliance with the terms set forth herein, ARINC may engage third parties to assist in any such data analytics of Pseudonymous Information.

2.11 Demonstrated Compliance. Upon prior written notice by the Customer, ARINC shall make available to the Customer all information necessary to demonstrate compliance with the terms set forth in this DPA including the verification of the procedures for the technical and organizational requirements of data protection and information security. ARINC shall promptly notify the Customer if, in the ARINC's opinion, the Customer's Processing instructions are in violation of Data Protection Laws.

2.12 Transfers of Personal Data.

2.12.1 Given the nature of the Services, it is possible that Personal Data may be transferred to other countries and/or Governmental Agencies that may not have the same Data Protection Laws as the country of original collection. Such transfer of Personal Data to third countries is necessary for the performance of contractual services for the Data Subject. Thus, for the purposes of establishing the appropriate safeguards in accordance with Data Protection Laws, the Parties hereby agree that the transfer of Personal Data is legitimized on the basis that such transfer is necessary for the performance of a contract for the Data Subject. This DPA constitutes Customer's instructions and agreement with respect to such transfers.

2.12.2 The Parties agree that if the Service Agreement involves any transfer of Personal Data from the countries in the European Economic Area ("EEA"), the United Kingdom (if not otherwise part of the EEA), and Switzerland (collectively "EEA/UK/CH"), then the Customer and ARINC agree that the terms of the Standard Contractual Clauses (the "SCCs") are incorporated herein by reference and the appropriate designations to the SCCs shall be set forth in Annex I (Exhibit 1-A) and Annex II (Exhibit 1-B), attached hereto and made a part

hereof. The Parties hereby agree to the following designations to the SCCs:

(a) The Parties agree that Module Two applies which reflects Customer serving as the Controller (data exporter) and ARINC serving as the Processor (data importer).

(b) For Module Two, Option 2 for Clause 9(a) of the SCCs applies, and notice shall be provided no less than 30 days in advance. However, where ARINC is using a sub-processor that goes out of business or there is some other emergency situation, ARINC shall: (i) provide as much notice as possible; and (ii) shall thereafter provide the Customer with 30 days to object and, if the Customer objects, identify an alternative sub-processor. The Customer agrees to make any objections in good faith. ARINC may provide notice by posting a list on a website that is communicated to the Customer in writing, by sending a written list to the Customer, or as otherwise agreed to in writing by the Parties.

(c) Option 2 for Clause 17 of the SCCs applies and the data exporter at issue shall be the relevant one. The law of Belgium shall be the governing law if the applicable EU Member State does not allow for third-party beneficiary rights.

(d) For clause 18 of the SCCs, disputes shall be resolved in the courts of the EU Member State for the relevant data exporter. If there are multiple relevant data exporters, the Parties agree to jurisdiction and forum of the courts of Belgium.

(e) If there is any conflict between the SCCs, the Services Agreement, this DPA, or any statement of work or order thereunder, the SCCs shall prevail.

(f) If the SCCs are modified by law or regulation (such as by action of the European Union), the Parties agree that, to the extent permitted by law, the modified version will automatically become effective and replace Exhibits 1A and 1B.

## 3. MISCELLANEOUS

3.1 Term. Unless as required by Data Protection Laws, this DPA shall cease to have any further effect upon, whichever is last to occur (i) the completion of the Services; or, (ii) to the extent applicable, the termination or expiration of a valid service agreement between ARINC and the Customer for the provision of the Services.

3.2 Amendments; Entire Agreement. The terms of this DPA shall supplement any and all services agreement(s) with respect to the provision of the Services by and between ARINC and the Customer. This DPA is the complete and exclusive statement of the agreement between the parties, which supersedes and merges all prior proposals, understandings and all other agreements, oral and written, between the parties relating to the subject matter of this DPA.

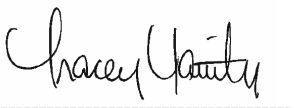
3.3 Severability. If any provision of this DPA shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from these terms and shall not affect the validity and enforceability of any remaining provisions of this DPA.

3.4 No Third Party Beneficiaries. Except with respect to the Data Subject rights set forth in the applicable Data Protection Laws, nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

3.5 Governing Law. The terms of this DPA shall be governed by the law of the member state in which the Data Exporter is established.

**IN WITNESS WHEREOF,** this DPA has been entered into as of the Effective Date.

Signed for and on behalf of **ARINC Incorporated** by: )

Signature 

**Authorised signatory**

Printed Name (block capitals) _____

**Tracey Yanity**

*ANNEX I: Exhibit 1A*

**Annex I to the Standard Contractual Clauses**

For purposes of this Annex I, "personal data" shall refer to the "personal data" that the data importer processes on behalf of the data exporter for the provision of products and services set forth in the DPA.

## A. LIST OF PARTIES

### A-1. Module Selection

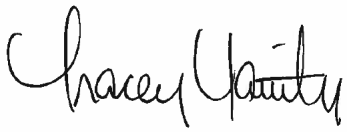
| Check which option(s) applies | |
|---|---|
| | **MODULE ONE: Transfer controller to controller** |
| X | **MODULE TWO: Transfer controller to processor** |
| | **MODULE THREE: Transfer processor to processor** |
| | **MODULE FOUR: Transfer processor to controller** |

### A-2. Data exporter(s):

| | |
|---|---|
| Company Name | Incorporated by reference from the Service Agreement |
| Company Address | Incorporated by reference from the Service Agreement |
| Company Role (Controller or Processor or Both) | Controller |
| Contact Person Name | See below |
| Contact Person Position/Title | Incorporated by reference from the Service Agreement |
| Contact Person Email and/or Telephone Number | Incorporated by reference from the Service Agreement |
| Description of the activities relevant to the data transferred by this company | Data exporter is using the services of the data importer for any one or more of the following: (1) managing airline and/or airport operations; (2) managing border security; (3) managing ticketing and reservations systems; (4) any other related personal data processing services or activities. |
| Name of person signing (does not need to be the contact) | Incorporated by reference from the Service Agreement |

| | |
|---|---|
| Title of person signing | Incorporated by reference from the Service Agreement |
| Signature | Incorporated by reference from the Service Agreement |
| Signature date | Incorporated by reference from the Service Agreement |

**A-3. Data importer(s):**

| | |
|---|---|
| Company Name | Incorporated by reference from the Service Agreement |
| Company Address | 2551 Riva Road, Annapolis, Maryland 21401 (USA) |
| Company Role (Controller or Processor or Both) | Processor |
| Contact Person Name | Data Privacy Office, OGC |
| Contact Person Position/Title | Lynne Kane-Van Reenan<br>Assistant General Counsel |
| Contact Person Email and/or Telephone Number | Lynne.kanevan@collins.com |
| Description of the activities relevant to the data transferred by this company | Data importer provides data communications transport services of any one or more of the following products and/or services: (1) global airport services; (2) business aviation services; and (3) commercial aviation services. |
| Name of person signing (does not need to be the contact) | Tracey Yanity |
| Title of person signing | Associate Director, Contracts |
| Signature |  |
| Signature date | Incorporated by reference from the Service Agreement |

B. **DESCRIPTION OF TRANSFER**

**B-1. Categories of data subjects whose personal data is transferred**

Data relating to individuals provided to data importer in providing any of its data communications services by the data exporter.

**B-2. Categories of personal data transferred**

The personal data transferred concern the following categories of data:

Any personal data required to allow data importer to perform the Services as set forth in the Services Agreement.

**B-3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

The personal data transferred concern the following special categories of data:

None, except where required by law to perform the Services set forth in the Services Agreement

**B-4. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).**

The frequency will be on an as-needed basis to support the work under the Services Agreement.

**B-5. Nature of the processing**

The nature of the Services being provided are set forth in the Service Agreement and any Statement of Work executed pursuant to, or Order issued under, the Services Agreement. The data importer will only process personal data for the purpose of providing those Services.

**B-6. Purpose(s) of the data transfer and further processing**

The data importer is a service provider for the data exporter. It will Process the data only to provide the Services under the Services Agreement.

**B-7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

Personal data shall be retained only so long as required to perform the Services under the Services Agreement and/or any Statement of Work executed pursuant to, or Order issued under, the Services Agreement.

**B-8. For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing**

Any transfers to sub-processors will be consistent with the terms of the Standard Contractual Clauses, the Section of the Terms and Conditions entitled “Data Privacy”, and this Annex I.

## C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13:*

Member State in which the relevant data exporter is established, which for the purposes of the Agreement will be considered the law of establishment of the relevant data controller.

*Exhibit 1B: ANNEX II*

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

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

The data importer undertakes to institute and maintain physical, technical, and organizational security measures in order to maintain and to protect the security of personal data created, collected, received, or otherwise obtained in connection with the Agreement, and the processing operations provided thereunder, which measures are required for the processing of personal data in accordance with the relevant data protection laws in the European Union.

The technical and organisational security measures of the data importer shall include, as a minimum, the following (as may be updated from time to time).

1. **Internal Controls and Systems**

The data importer will implement security rules in the form of mandatory policies and procedures for staff and all subcontractors or agents who have access to customer personal data. These policies and procedures cover:

- measures, standards, procedures, rules and norms to address the appropriate level of security;
- the meaning and importance of personal data and the need to keep it secure, confidential and accessed on a need to know basis only;
- staff functions, obligations and access rights;
- the procedures for reporting, managing and responding to personal data security incidents; and
- the procedures for making backup copies and recovering personal data.

2. **Security**

Access to personal data by the data importer is provided through access and procedures. The following summarizes key security obligations:

**a. Functions and obligations of staff with regards to data files:**

Where required, the functions and obligations of each of the users or profiles of users with access to the personal data and to the information systems must be clearly defined in writing (i.e., procedures, policies or related contractual obligations).

**b. Record of incidents:**

There shall be a procedure for notification and management of incidents that affect personal data and a register established for recording the type of incident, the moment it occurred, or if appropriate, was detected, the person making the notification, to whom it was communicated, the effect arising from it and the corrective measures applied.

**c. Identification and Authentication:**

The data importer shall take the measures that ensures the identification and authentication of the users. The data importer shall establish a mechanism that permits the identification of any user who tries to access the information system and the verification of his authorization. The data importer's documentation shall establish the frequency, which under no circumstances shall be less than yearly, with which the passwords shall be changed. While in force, passwords shall be stored in an unintelligible way.

**d. Backup Copies and Recovery:**

The data importer shall ensure that: (1) backups are created at least weekly, unless otherwise defined; and (2) data recovery procedures are implemented that enable their reconstruction to the original state at the moment the loss or destruction occurred, to the extent technically feasible.

**e. Responsible Personnel:**

The data importer shall appoint one or several privacy officers, to the extent regulatorily required, and security personnel responsible for creating, implementing and monitoring compliance with the policies and procedures. This appointment may be structured across a region for all of the data importer's product and service processing systems or across a specific products and services group.

**f. Audit:**

The data importer shall ensure that an internal or external audit is conducted that verifies compliance with its privacy and security measures outlined in its policies and procedures.

**g. Access Controls:**

The data importer's policies and procedures shall require and the data importer shall establish a mechanism to limit unauthorized access to the data.

**h. Physical access control:**

The data importer's policies and procedures shall require and the data importer shall ensure that only the personnel authorized have access to the places housing the physical equipment that supports the information systems.

***Exhibit 1C: ANNEX III***

**LIST OF SUB-PROCESSORS**

***OMITTED / NOT APPLICABLE***

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

| | | | |
|---|---|---|---|
| Company Name | | | |
| Company Address | | | |
| Company Role (Controller or Processor or Both) | | | |
| Contact Person Name | | | |
| Contact Person Position/Title | | | |
| Contact Person Email and/or Telephone Number | | | |
| Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised) | | | |