DATA PROCESSING AND TRANSFER AGREEMENT
For Independent Controllers / Processors (Combined)

This Data Processing and Transfer Agreement ("DPTA") shall be effective on the same date as the Purchase Order, Order Confirmation or Purchasing or Service Agreement ("Agreement"), or at the latest upon the signature of this DPTA, and supplements the Agreement with respect to the Services provided therein by and between

_____

[name **German legal entity of Collins Aerospace]**, an RTX Business, (the "Buyer" or "Collins"), and

_____

[insert **Supplier** name and address as defined in the Agreement] and its subsidiaries and affiliates (collectively "Supplier").

This DPTA shall control the exchange of Personal Information between the parties and be incorporated into all agreements between the parties.

Capitalized terms in this DPTA shall have the meanings ascribed to such terms under paragraph 1 (or in other locations throughout this DPTA or the Agreement), and, if not otherwise defined, shall have their ordinary and customary meanings.

1. The following definitions are applicable to this provision:

   (a) "Business Activities" and/or "Services" shall mean the services and work performed under any Agreements subject to this DPTA.

   (b) "Data Privacy Laws" shall mean applicable national, federal, state and provincial laws relating to data privacy, the protection of personal information or data, and the cross-border transfer of personal information or data, including, without limitation, the General Data Protection Regulation ("GDPR") and any law or regulation that may be enacted to implement or replace the GDPR.

   (c) "Personal Information" shall mean any information or data provided to by Collins or Supplier or their agents, representatives, or subcontractors in connection with the Business Activities and that relates to any identified or identifiable natural person, or, to the extent of a conflict with applicable law, that is subject to any Data Privacy Laws.

   (d) The terms "controller," "data subject," "processor" and "process" (including grammatical variations) shall have the meaning provided in the GDPR.

2. With respect to the Business Activities, Collins shall have the responsibility of acting as the controller of the Collins Personal Information in its possession, custody, or control, and the Supplier shall have the responsibility of acting as an independent controller and/or processor of the Collins Personal Information.

3. To the extent the parties are each acting as **independent controllers**, each party shall:

   (a) comply with all applicable Data Privacy Laws related to the Personal Information

provided by the other party;

(b) provide an appropriate privacy notice and/or consent to the data subjects whose Personal Information that party Processes in the course of the Business Activities. Each party is responsible for providing a privacy notice regarding the Processing for which that party is responsible. Where Collins provides Collins Personal Information and Supplier anonymizes the data and Processes it anonymously only, the parties agree that Collins is responsible for providing the notice or consent;

(c) address requests received from data subjects seeking to access, correct, delete, or object to the Processing of Collins Personal Information in the context of the Business Activities. While each party shall be responsible for addressing those requests that it receives, the parties recognize that there may be circumstances requiring that they work together, such as where one party has a database, system, or other technology that uniquely allows for the access, correction, deletion, or objection that the data subject seeks. In these circumstances, the parties agree to notify the other party in writing and to take reasonable commercial efforts to work together; and

(d) provide such information, assistance and cooperation as the other party or its Affiliates may reasonably require from time to time establishing compliance with Data Privacy Laws.

4. To the extent **Supplier is acting as a processor**, Supplier shall:

(a) only collect, access, use, or share Collins Personal Information, or transfer Collins Personal Information to authorized third parties, in performance of the Business Activities (including auditing of Business Activities) or to comply with legal obligations. Supplier will not make any secondary or other use (e.g., for the purpose of data mining) of Collins Personal Information except (a) as expressly authorized in writing by the Agreement or otherwise by Collins, or (b) as required by law;

(b) not share with, transfer to, disclose or provide access to Collins Personal Information to any third party except to facilitate or assist in the Business Activities or as required by law. If either party does share, transfer, disclose or provide access to Collins Personal Information to a third party, it shall:

(i) be responsible for the acts and omissions of any subcontractor or other third party, that processes (within the meaning of the applicable Data Privacy Laws) Collins Personal Information in the same manner and to the same extent as it is responsible for its own acts and omissions with respect to such Collins Personal Information;

(ii) ensure such third party is bound by a written agreement that contains the same or equivalent obligations and protections as those set forth in this Section; and

(iii) only share, transfer, disclose or provide access to a third party to the extent that such conduct is compliant with applicable law;

This section 4(b) does not address sharing with, or transferring, disclosing, or providing access to, one or more government entities pursuant to a legal obligation. Such conduct shall be done in a manner intended to protect and limit the sharing of Collins Personal Information to the extent reasonably and legally permissible.

(c) take commercially reasonable steps to ensure the reliability of its employees, agents, representatives, subcontractors, subcontractor employees, or any other person used who have access to the Collins Personal Information (collectively, "Personnel"), ensure that such access is on a need-to-know basis including the establishment of confidentiality agreements as appropriate, and ensure that Personnel are obligated to maintain the confidentiality of Collins Personal Information, such as through a confidentiality agreement or by application of company policy, relevant law or regulation;

(d) maintain reasonable and appropriate technical, physical, and administrative safeguards intended to protect Collins Personal Information. These measures will include reasonable restrictions upon physical access to any locations containing Collins Personal Information, such as the storage of records in locked facilities, storage areas, or containers. Supplier must periodically re-evaluate the measures adopted to ensure that the remain reasonable and appropriate;

(e) provide Collins with commercially reasonably assistance in: (i) deleting Collins Personal Information upon request by a data subject or legal representative where appropriate; and (ii) managing requests from data subjects that wish to opt-out when applicable;

(f) retain Collins Personal Information only for as long as required and thereafter purge Collins Personal Information unless otherwise required to retain the data by applicable law;

(g) immediately advise Collins in writing if Supplier receives or learns of any:

(i) complaint or allegation indicating a violation of Data Privacy Laws regarding the Collins Personal Information;

(ii) inquiry or complaint from one or more data subjects relating to the Processing of Collins Personal Information; and

(iii) any regulatory request for, subpoena, search warrant, or other legal, regulatory, administrative, or governmental process seeking Collins Personal Information (collectively, "Data Privacy Matters"). If Supplier learns of any Data Privacy Matter, Supplier shall, in addition to notifying Collins in writing, provide reasonable assistance to Collins, including by cooperating with Collins in investigating the Data Privacy Matter, providing relevant information to Collins, assisting in the preparation of a response, implementing a remedy, and/or cooperating in the conduct of and defending against any claim, court or regulatory proceedings. Supplier shall use commercially and legally reasonable efforts to limit the nature and scope of any required disclosure to the minimum amount of Collins Personal Information required to comply with applicable law. Unless prevented by applicable law, Supplier shall provide Collins with advance written notice of any Data Privacy Matters sufficient to allow Collins to contest any legal, regulatory, administrative, or other governmental processes; and

(h) provide written notice to Collins as soon as possible and, whenever possible in forty-eight (48) hours, of any incident of accidental or unlawful destruction or accidental loss, alteration, unauthorized or accidental disclosure of or access to Collins Personal Information of which it becomes aware (a "Security Breach").

Supplier, as the Controller, shall be responsible for the investigation and remediation of the Security Breach. Notwithstanding the foregoing, Supplier shall obtain Collins's prior written consent before making any notification to a regulator, the public, other customers, or affected individuals that identifies Collins, except where Supplier makes a diligent effort to obtain Collins's consent and Supplier is required to make a notification pursuant to a legal obligation.

5. If the Data Privacy Laws shall be amended, the parties shall work together to make any required amendments to this DPTA. The parties shall take commercially reasonable efforts to procure each third party to make those or comparable amendments.

6. Data Transfers.

If the Agreement involves the provision of Business Activities where the Supplier will transfer Collins Personal Information from any country in the European Economic Area, the United Kingdom or Switzerland (collectively, "EEA/UK/CH") to outside the EEA/UK/CH that do not have an adequacy decision, then Collins and Supplier agree that the Standard Contractual Clauses adopted by the European Commission in Decision 2021/914/EU (hereinafter the "SCCs") are incorporated by reference as if set forth herein. In addition, transfers from the UK to locations outside the UK that do not have an adequacy decision shall also be governed by the 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 s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, which are incorporated by reference as if set forth herein (hereinafter "UK Mandatory Clauses"). In furtherance of the foregoing, Collins and Supplier agree that:

a. The parties agree that the Supplier will act as either an independent controller and/or processor in which case, the Parties agree that either "***Module One***" and/or "***Module Two***" applies.

b. For **Clause 9(a) [Use of sub-processors]**, Option 2 [general written authorization] applies and notice shall be provided no less than 30 days in advance. However, where Supplier is using a sub-processor that goes out of business or there is some other emergency situation, Supplier shall: (i) provide as much notice as possible; (ii) take commercially reasonable efforts to ensure that the sub-processor is not a competitor of Collins; and (iii) thereafter provide Collins with 30 days to object and, if Collins objects, identify an alternative sub-processor. Collins agrees to make any objections in good faith. Supplier may provide notice by posting a list on a website that is communicated to Collins in writing, by sending a written list to Collins, or as otherwise agreed to in writing by the Parties.

c. For **Clause 17** (Option 2) **[Governing law]**, except for transfers from the UK, which shall be governed by the law of England and Wales, 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 [Choice of forum and jurisdiction]**, 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, except for disputes arising solely out of a transfer from the UK, for which the parties agree to the jurisdiction and forum of the courts of England and Wales.

e. Annexes I and II of the SCCs are attached hereto as Exhibit 1A and 1B, respectively. Annex III is not applicable.

f. If there is any conflict between the SCCs (as modified by the UK Mandatory Clauses where applicable) and the Agreement or any statement of work or order thereunder, the SCCs shall prevail.

g. If the Standard Contractual Clauses 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 Exhibit 1.

7. If the Agreement involves collection or processing of Collins Personal Information from data subjects in California, then the parties agree that Supplier is a "Service Provider", as such term is defined in the California Consumer Privacy Act, Cal, Civ. Code §§ 1798.100 et. seq. (the "CCPA") (and regulations implementing, revising, or replacing CCPA), and will neither sell, nor exchange for anything of value, Collins Personal Information. If the Agreement does not involve collection or processing of Collins Personal Information from data subjects in California, then this section 7 does not apply.

Exhibit 1A: ANNEX I

Annex I to the Standard Contractual Clauses

For purposes of this Annex I, "personal data" shall include Buyer Personal Information.

A. LIST OF PARTIES

A-1. Module Selection

Check which option(s) applies	
X	**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): German legal entity of Collins Aerospace, an RTX Business

Company Name	
Company Address	
Company Role (Controller or Processor or Both)	Controller
Contact Person Name	See below
Contact Person Position/Title	Chief Privacy Officer
Contact Person Email and/or Telephone Number	Privacy.compliance@rtx.com + (011) 781-522-3000
Description of the activities relevant to the data transferred by this company	The Services as described in the Agreement, in the course of receiving the Services, the data exporter will need to share personal data as set forth in Section B below.
Name of person signing (does not need to be the contact)	
Title of person signing	
Signature	
Signature date	

A-3. Data importer(s): Supplier / Service Provider

Company Name	
Company Address	
Company Role (Controller or Processor or Both)	Controller / Processor
Contact Person Name	
Contact Person Position/Title	
Contact Person Email and/or Telephone Number	
Description of the activities relevant to the data transferred by this company	
Name of person signing (does not need to be the contact)	
Title of person signing	
Signature	
Signature date	

B. DESCRIPTION OF TRANSFER

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

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

- employees, contractors, customers, end users, job applicants, and investors
- Personnel of Collins' business partners, such as vendors, suppliers, and customers
- Third parties whose personal data Collins may have for legal reasons, such as parties in litigation

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 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 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 Agreement.

B-5. Nature of the processing

The nature of the Services being provided are set forth in the Agreement and any Statement of Work executed pursuant to, or Order issued under, the 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 importers are service providers for Collins. They will Process the data only to provide the Services under the 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 Agreement and/or any Statement of Work executed pursuant to, or Order issued under, the 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 (Supervision) of the SCCs:

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

X MODULE ONE: Transfer controller to controller

X 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).

Internal Controls and systems

The data importer shall comply with strict internal controls in line with ISO 27001 and ISO 20000 guidelines. 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 RTX group 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.

Security

Access to personal data by the data importer is provided through access and procedures governed by RTX.
The following summarizes key security obligations (and in the event of dispute or inconsistency, the fuller security obligations agreed shall prevail):

Functions and obligations of staff with regards to data files:

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 in a security document.

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.

Identification and Authentication:

The data importer shall take the measures that guarantee the correct identification and authentication of the users. The data importer shall establish a mechanism that permits the unequivocal and personalized identification of any user who tries to access the information system and the verification of his authorization. The security document 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.

Backup Copies and Recovery:

The security document shall require and the data importer shall ensure that: (1) backups are created at least weekly; 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.

Security Officer:

The security document shall appoint one or several security officers responsible for implementing and monitoring compliance with the requirements of the security document. This appointment may be general for all the filing systems or processing of personal data or specific depending on the information systems used, which shall be clearly recorded in the security document.

Audit:

The security document shall require and the data importer shall ensure that, at least every two years, an internal or external audit is conducted that verifies compliance with the security measures contained in the security document.

Management of Media and Documents:

The security document shall require and the data importer shall ensure that a registration or inventory system for the entry of media containing Data shall be established permitting, directly or indirectly, identification of the type of document or media, as well as the date and time, the issuer, the number of documents or media included in the transmission, the type of information they contain, the method of transmission and the person responsible for receipt.

Identification and Authentication:

The security document shall require and the data importer shall establish a mechanism to limit unauthorized access to the Data, including updating the security document based on new or newly identified risks.

Physical Access Control:

The security document 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.

Record of Recovery of Incidents:

The register shall provide the procedures for the recovery of data, indicating the person who executed the process, the data restored and, if appropriate, which data have had to be manually recorded in the recovery process.