

DATA PROCESSING AND TRANSFER AGREEMENT

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

[insert name and address of Collins Aerospace German company] and its subsidiaries and affiliates (in the following "Collins Aerospace"), and

[insert company name and address] (in the following, "Supplier").

1. This DPTA shall apply to any and all Agreements. Except as expressly supplemented by this DPTA with respect to the subject matter hereunder, the terms of each Agreement shall continue unchanged and shall apply with full force and effect as to the matters addressed therein. This DPTA is hereby incorporated into and forms a part of any such Agreement.

Capitalized terms in this DPTA shall have the meanings ascribed to such terms under Section 2 (or in other locations throughout this DPTA), and, if not otherwise defined, shall have their ordinary and customary meanings.

This DPTA will supersede any previous agreements between the parties as to the subject matter herein, including all prior data transfer agreements entered into between Collins Aerospace and Supplier pursuant to European Union Directive 95/46/EC.

2. The following definitions are applicable to this DPTA:
 - (a) "Agreement" shall mean any agreement entered into between Collins Aerospace and Supplier before, on or after the Effective Date, including any orders, releases, statements of work or the like issued or entered into pursuant thereto.
 - (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 laws and regulations of the European Union member states under the General Data Protection Regulation ("GDPR") and any European Union law or regulation that may be enacted to implement or replace the GDPR.
 - (c) "Personal Data" shall mean any information or data provided to Supplier or its agents, representatives, or subcontractors in connection with the Agreement, and the transactions thereunder that relate 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 "processing" (including grammatical variations) shall have the meaning set out in the GDPR.
3. Supplier shall:
 - (a) comply with all applicable Data Privacy Laws and promptly notify Collins Aerospace in writing if Supplier believes that collecting or processing Collins Aerospace Personal Data violates Data Privacy Laws;
 - (b) only collect, access, use, or share Collins Aerospace Personal Data, or transfer Collins Aerospace Personal Data to authorized third parties, in performance of its obligations under the Agreement, in conformance with Collins Aerospace's instructions, 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 Aerospace Personal Data except (i) as expressly authorized in writing by Collins Aerospace, (ii) as required by law;
 - (c) not share, transfer, disclose or provide access to Collins Aerospace Personal Data to any third party except to provide services under the Agreement or as required by law. If Supplier does share, transfer, disclose or provide access to Collins Aerospace Personal Data to a subcontractor or sub-processor, it shall:
 - (i) be responsible for the acts and omissions of any subcontractor or other such

- third party, that processes (within the meaning of the applicable Data Privacy Laws) Collins Aerospace Personal Data on Supplier's behalf in the same manner and to the same extent as it is responsible for its own acts and omissions with respect to such Collins Aerospace Personal Data;
- (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 Data Privacy Laws;
- (d) not appoint (or disclose any Company Personal Data to) any sub-processor unless required or authorized by the Company;
 - (e) take commercially reasonable steps to ensure the reliability of Supplier's employees, agents, representatives, subcontractors, subcontractor employees, or any other person used by Supplier (collectively, "Supplier Personnel") who have access to the Collins Aerospace Personal Data and ensure that Supplier Personnel are obligated to maintain the confidentiality of Collins Aerospace Personal Data, such as through a confidentiality agreement or by application of relevant law or regulation;
 - (f) provide such information, assistance and cooperation as Collins Aerospace may reasonably require from time to time to establish Supplier's compliance with Data Privacy Laws,
 - (g) upon Collins Aerospace's request, permit Collins Aerospace to hire third party external auditors to verify Supplier and third party compliance with their obligations under this DPTA. Additionally, upon request, Supplier shall provide Collins Aerospace with any audit reports issued (if any) under ISO 27001, ISO 29100, SSAE 16 (or SAS 70), SSAE 18, SOC 2, OR ISAE 3402 that covers Collins Aerospace Personal Data;
 - (h) will maintain reasonable and appropriate technical, physical, and administrative safeguards intended to protect Collins Aerospace Personal Data. These measures will include reasonable restrictions upon physical access to any locations containing Collins Aerospace Personal Data, such as the storage of such records in locked facilities, storage areas, or containers. Supplier shall share specifics of its technical and organizational measures in order to enable Collins Aerospace to evaluate the security of its data. Supplier must periodically re-evaluate the measures adopted to ensure that they remain reasonable and appropriate;
 - (i) provide Collins Aerospace with commercially reasonable assistance in:
 - (i) deleting Collins Aerospace Personal Data in response to a request by an individual or legal representative; and
 - (ii) enabling individuals to opt-out, pursuant to Collins Aerospace's written instructions;
 - (j) provide a privacy notice to individuals with whom the Supplier has direct contact unless Supplier and Collins Aerospace agree in writing that the privacy notice obligation is solely Collins Aerospace's responsibility;
 - (k) pursuant to Collins Aerospace's written instructions, provide Collins Aerospace with the ability to purge Collins Aerospace Personal Data older than one year or such other time period agreed upon in writing by the parties, unless otherwise required to retain the data by applicable law; and
 - (l) immediately advise Collins Aerospace in writing if it receives or learns of any:
 - (i) complaint or allegation indicating a violation of Data Privacy Laws regarding Collins Aerospace Personal Data;
 - (ii) request from one or more individuals seeking to access, correct, or delete Collins Aerospace Personal Data;
 - (iii) inquiry or complaint from one or more individuals relating to the collection, processing, use, or transfer of Collins Aerospace Personal Data; and
 - (iv) regulatory request for, subpoena, search warrant, or other legal, regulatory, administrative, or governmental process seeking Collins Aerospace Personal Data

(collectively, "Data Privacy Matters"). If Supplier learns of any Data Privacy Matters, Supplier shall provide assistance to Collins Aerospace, fully cooperate with Collins Aerospace in investigating the matter, including but not limited to, providing the relevant information to Collins Aerospace, preparing a response, implementing a remedy, and/or cooperating in the conduct of and defending against any claim, court or regulatory proceedings. Collins Aerospace shall be responsible for communicating with individuals regarding their Collins Aerospace Personal Data in connection with such Data Privacy Matters unless Collins Aerospace authorizes Supplier to do so on its behalf. Supplier shall use commercially and legally reasonable efforts to limit the nature and scope of the required disclosure to the minimum amount of Collins Aerospace Personal Data required to comply with applicable law. Unless prevented by applicable law, Supplier shall provide Collins Aerospace with advance written notice of any such Data Privacy Matters sufficient to allow Collins Aerospace to contest legal, regulatory, administrative, or other governmental processes.

4. Supplier shall provide written notice to Collins Aerospace as soon as possible and, whenever possible, in forty-eight (48) hours, of any actual or reasonably suspected incident of accidental or unlawful destruction or accidental loss, alteration, unauthorized or accidental disclosure of or access to Collins Aerospace Personal Data of which it becomes aware (a "Security Breach"). If Supplier is unable to provide notice within forty-eight (48) hours, Supplier shall provide Collins Aerospace with an explanation for the delay that Collins Aerospace will be entitled to share with regulators. Supplier shall take all reasonable measures to contain and remedy the Security Breach, wherever possible; provide Collins Aerospace with information regarding the investigation and remediation of the Security Breach, unless restricted by law; not make any notification, announcement or publish or otherwise authorize any broadcast of any notice or information about a Security Breach (a "Breach Notice") without the prior written consent of and prior written approval by Collins Aerospace of the content, media and timing of the Breach Notice (if any), unless required to do so by law or court order; and even where required to do so by law or court order, make all reasonable efforts to coordinate with Collins Aerospace prior to providing any Breach Notice. Where the Security Breach (a) involves data on the Supplier's networks or systems or (b) is the fault of the Supplier, then Supplier will, at the request of Collins Aerospace, pay for the costs of remediation, notification (including, where reasonably necessary, a call center), and, if the Security Breach involves data elements that could lead to identity theft, provide the affected individuals with credit monitoring or other commercially-reasonable identity theft mitigation service for one year or such longer period as required by law or a government regulator.
5. In the event Supplier shall provide to Collins Aerospace personal information protected by Data Privacy Laws, Supplier shall ensure that such personal information is provided consistent with applicable law, including, where required, obtaining consent or providing notice.
6. All Collins Aerospace Personal Data acquired by Supplier shall be returned or destroyed (at the option of Collins Aerospace), unless and to the extent that: (i) such Collins Aerospace Personal Data is required by Supplier to discharge its obligations hereunder or under applicable law; or (ii) return or destruction is prohibited by applicable law. Absent contrary instructions and except as prohibited by law, Supplier shall immediately destroy all Collins Aerospace Personal Data after termination or completion of the statement of work after waiting 30 days to allow Collins Aerospace to request return of Collins Aerospace Personal Data.
7. If the Agreement involves collection or Processing of Collins Aerospace Personal Information from individuals 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. and implementing regulations (the "CCPA"), and will neither sell, nor exchange for anything of value, Collins Aerospace Personal Information.
8. The parties agree that any transfer of Collins Aerospace 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") shall be pursuant to the "Standard Contractual Clauses" (Exhibit 1) of the European Union according to the EU Directive 2016/679 and the Decision of the European Commission 2021/914 in instances in which the Supplier serves as a Processor for Collins Aerospace.

9. Governing law and choice of forum provisions from the Agreement shall apply to the DPTA, except for Standard Contractual Clauses (SCC) if signed. SCC shall be governed by the law of the Member State in which the data exporter is established, which for the purposes of this DPTA will be considered the law of establishment of the relevant data controller.
10. In the event of any conflict or inconsistency between the provisions of this DPTA, SCC, and an Agreement, such conflict or inconsistency shall be resolved by giving precedence to the provision in the following order of priority:
 - (i) Section 11 of this DPTA;
 - (ii) the terms of Appendices and Exhibits (Standard Contractual Clauses if required and signed) to this DPTA;
 - (iii) this DPTA (other than Section 11); and
 - (iv) the Agreement(s) between Collins Aerospace and Supplier.
11. This DPTA, including SCC, if required, and the Appendices thereto, may be executed electronically and in multiple counterparts, each of which will be considered an original, and all of which, when taken together, will constitute one agreement binding on the parties, even if both parties are not signatories to the original or the same counterpart.

Rockwell Collins Deutschland GmbH

_____ *[company name]*

Signature

Signature

Name

Name

Position

Position

Signature

Signature

Name

Name

Position

Position

Date: _____

Enclosures:

Appendix 1 – Processing Activities

Appendix 2 – Technical and Organizational Measures

Appendix 3 – Authorised Sub-Processors

APPENDIX 1 – Processing Activities

Data exporter (Controller)

_____ [German Collins Aerospace company name]

Data Protection Officer

Privacy Officer

E-Mail: Privacy.compliance@rtx.com oder martina.weber-bauer@collins.com

Data importer (Processor)

_____ [Supplier name]

Data Protection Officer of Processor

Der Datenschutzbeauftragte des Auftragsbearbeiters kann wie folgt kontaktiert werden:

_____ [Contact details]

Data Subjects

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

Categories of Data

The personal data transferred concern the following categories of data:

Special Categories of Data (if appropriate)

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

Processing Operations

The personal data transferred will be subject to the following basic processing activities:

APPENDIX 2 – TECHNICAL AND ORGANIZATIONAL MEASURES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

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 Collins Aerospace 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 Collins Aerospace.

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.

APPENDIX 3: AUTHORISED SUB-PROCESSORS

List of Authorized Subprocessors as at the Agreement Signature Date to be included here.

_____ *[company or person name]*

_____ *[address, seat]*

_____ *[describe type of sub-processing]*