



**AMENDMENT**  
**EU/UK Standard Contractual Clauses**

This Amendment (“**Amendment**”) effective as of January 1, 2022 (the “**Amendment Effective Date**”), is entered into by and between Goodrich Corporation, Hamilton Sundstrand Corporation and Rockwell Collins, Inc., each a part of Collins Aerospace, and their respective subsidiaries and affiliates (hereinafter collectively referred to as “**Collins**”) and the company referenced hereinbelow (including its subsidiaries and affiliates) (collectively, the “**Supplier**”). This Amendment refers to Collins and the Supplier collectively as the “**Parties**” and individually, as a “**Party**”.

**RECITALS**

**WHEREAS**, Collins and Supplier have executed one or more agreements (including without limitation, statements of work or orders) together with all prior amendments, modifications revisions, and/or associated data processing agreements (collectively, the “**Agreement(s)**”) whereby the Supplier provides related products and services to Collins (the “**Services**”);

**WHEREAS**, in its delivery of such Services, the Supplier may process personal data on Collins’s behalf and/or pursuant to Collins’s instructions;

**NOW THEREFORE**, the Parties mutually agree as follows:

- 1) **Amendments**. The Agreement is hereby amended by adding the below clause, which such clause shall amend and replace in its entirety any such existing clause in the Agreement that pertains to the cross-border transfers of personal data from the countries set forth in the below clause:

**Data Transfers**. If the Agreement involves the provision of Services where the Supplier will transfer Collins personal data 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 as designated in the Agreement, in which case, the Parties agree that either “**Module One**” and/or “**Module Two**” applies.
- b. For Clause 9(a), Option 2 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.

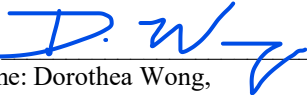
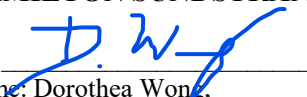
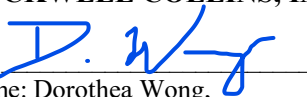


# Collins Aerospace

- c. For clause 17 (Option 2) applies. 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, 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.

- 2) **Defined Terms.** All capitalized terms used herein but not otherwise defined herein shall have the meanings ascribed to them in the Agreement.
- 3) **No Further Amendments.** Except as expressly set forth herein, the Agreement remains unmodified and in full force and effect.

IN WITNESS WHEREOF, the Parties have caused this Amendment to be executed as of the Amendment Effective Date.

<p><b>SUPPLIER:</b></p> <p><i>[Incorporated by reference from Collins Aerospace DPA Portal registration page]</i></p>	<p><b>COLLINS: GOODRICH CORPORATION</b></p> <p>By: <u></u>  Name: Dorothea Wong,  Title: Executive Director, Indirect Supply Chain,  Collins Aerospace 07/18/22</p> <p><b>HAMILTON SUNDSTRAND CORPORATION</b></p> <p>By: <u></u>  Name: Dorothea Wong,  Title: Executive Director, Indirect Supply Chain,  Collins Aerospace 07/18/22</p> <p><b>ROCKWELL COLLINS, INC.</b></p> <p>By: <u></u>  Name: Dorothea Wong,  Title: Executive Director, Indirect Supply Chain,  Collins Aerospace 07/18/22</p>
---	--



**Exhibit 1A: ANNEX I**

**ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES**

**FOR PURPOSES OF THIS ANNEX I, “PERSONAL DATA” SHALL INCLUDE COLLINS PERSONAL INFORMATION.**

**A. LIST OF PARTIES**

**A-1. Module Selection**

Check which option(s) applies	
X	<b>MODULE ONE: Transfer controller to controller</b>
X	<b>MODULE TWO: Transfer controller to processor</b>
	<b>MODULE THREE: Transfer processor to processor</b>
	<b>MODULE FOUR: Transfer processor to controller</b>

**A-2. Data exporter(s):** Goodrich Corporation, Hamilton Sundstrand Corporation and Rockwell Collins, Inc., each a part of Collins Aerospace, and their respective subsidiaries and affiliates (hereinafter collectively referred to as “**Collins**”)

Company Name	Company name from the Amendment
Company Address	Company address from the Amendment
Company Role (Controller or Processor or Both)	Controller
Contact Person Name	Data Privacy Office
Contact Person Position/Title	Privacy Officer
Contact Person Email and/or Telephone Number	dataprivacy@collins.com
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 below.
Name of person signing (does not need to be the contact)	Incorporated by reference from the Amendment
Title of person signing	Incorporated by reference from the Amendment
Signature	Incorporated by reference from the Amendment
Signature date	Effective date as specified in the Amendment



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

Company Name	<i>Incorporated by reference from Collins Aerospace DPA Portal registration page</i>
Company Address	<i>Incorporated by reference from Collins Aerospace DPA Portal registration page</i>
Company Role (Controller or Processor or Both)	Controller / Processor
Contact Person Name	To be supplied upon request
Contact Person Position/Title	To be supplied upon request
Contact Person Email and/or Telephone Number	To be supplied upon request
Description of the activities relevant to the data transferred by this company	Providing the Services as covered in the Agreement
Name of person signing (does not need to be the contact)	<i>Incorporated by reference from Collins Aerospace DPA Portal registration page</i>
Title of person signing	<i>Incorporated by reference from Collins Aerospace DPA Portal registration page</i>
Signature	<i>Incorporated by reference from Collins Aerospace DPA Portal registration page</i>
Signature date	Effective date as specified in the Amendment

**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:

- Collins employees, contractors, customers, end users, job applicants, and investors
- Personnel of Collins’s 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. 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.

**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**

Check which option(s) applies	
X	<b>MODULE ONE: Transfer controller to controller</b>
X	<b>MODULE TWO: Transfer controller to processor</b>
	<b>MODULE THREE: Transfer processor to processor</b>

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 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 the data exporter.

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 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.