

Data Processing and Transfer Agreement

This Data Processing and Transfer Agreement (“DPTA”) effective as of the effective date of the agreement (“Agreement”) between RTX and Supplier (“Effective Date”), is entered into between ARINC Incorporated (a part of Collins Aerospace) and its subsidiaries and affiliates (collectively, “Buyer” or “RTX”), and the supplier and its subsidiaries and affiliates (collectively, “Supplier”).

WHEREAS, RTX and Supplier have entered into an agreement (“**Service Agreement**”) under which Supplier will provide certain goods or perform certain services on for or on behalf of RTX;

WHEREAS, in performing such services, Supplier may be processing Personal Data as part of delivering the services;

WHEREAS, it is therefore necessary for the parties to enter into an appropriate data processing agreement which reflects the roles of the parties and their obligations under the applicable Data Protection Laws and the Parties wish to enter into this DPA.

NOW, THEREFORE, the parties agree as follows:

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 “Buyer Personal Information” means any information or data provided (directly or indirectly) or made accessible to Supplier or its agents, representatives, or subcontractors in connection with a Service Agreement or any Order 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.

1.2 “Data Privacy Laws” means 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.

1.3 “Order” means Buyer’s purchase order, in either paper or electronic form, sent by Buyer to Supplier, to initiate the ordering of Services, including modifications thereto. The phrase “in connection with the Order” includes performance of the Order, performance in anticipation of the Order, and

preparation of a bid or proposal for the Order. Where the context permits, the term Order includes Service Agreement.

1.4 “Process” means with respect to RTX Information, to use, access, manipulate, modify, disclose, store (including backup), transmit, transfer, retain and dispose of such RTX Information.

1.5 “RTX” means Raytheon Technologies Corporation.

1.6 “RTX Information” means (i) any Proprietary Information and any other data, materials, or information owned or managed by Buyer or Buyer’s Affiliates or which Buyer or Buyer’s Affiliates are obligated to manage and/or protect on behalf of others: (a) provided to Supplier by Buyer or Buyer’s Affiliate; or (b) that Supplier collects, Processes, generates, or uses for or on behalf of or at the direction of Buyer or Buyer’s Affiliate in providing the Services to Buyer or Buyer’s Affiliate; or (c) collected, Processed, generated, or used by Supplier or Supplier Personnel in providing the Services, including in each case metadata from Buyer’s or Buyer’s Affiliates’ use of the Services and derivatives of any of the foregoing (e.g., aggregations of RTX Information, profiles of users of the Services, or analysis of the content of Buyer or Buyer’s Affiliate data records or how Buyer or Buyer’s Affiliate uses the Services) and (ii) Buyer Personal Information.

1.7 “Supplier Personnel” means Supplier’s employees, agents, representatives, subcontractors, subcontractor employees, or any person used by Supplier in the performance under a contract with RTX.

2. PROCESSOR OBLIGATIONS

2.1 Supplier shall:

2.1.1 comply with all applicable Data Privacy Laws and promptly notify Buyer in writing if Supplier believes that collecting or Processing Buyer Personal Information pursuant to this Section (including subparts) infringes Data Privacy Laws;

2.1.2 only collect, access, use, or share Buyer Personal Information, or transfer Buyer Personal Information to authorized third parties, in performance of its obligations under the Service Agreement and/or Order(s) issued thereunder, in conformance with Buyer’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 Buyer Personal Information except (i) as

expressly authorized in writing by Buyer, or (ii) as required by law;

2.1.3 not allow any third party to Process Buyer Personal Information except to provide services under the Service Agreement and/or Order or as required by law. If Supplier does allow a third party to Process Buyer Personal Information, Supplier shall:

2.1.3.1 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) Buyer Personal Information 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 Buyer Personal Information;

2.1.3.2 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

2.1.3.3 only share, transfer, disclose, or provide access to a third party to the extent that such conduct is compliant with applicable Data Privacy Laws;

2.1.4 take commercially reasonable steps to ensure: (i) the reliability of Supplier Personnel who have access to the Buyer Personal Information; (ii) that access to Buyer Personal Information by Supplier Personnel is on a need-to-know basis; (iii) and that Supplier Personnel are obligated to maintain the confidentiality of Buyer Personal Information, such as through a confidentiality agreement or by application of relevant law or regulation;

2.1.5 provide such information, assistance, and cooperation as Buyer may reasonably require from time to time to establish Supplier's compliance with Data Privacy Laws;

2.1.6 upon Buyer's request, permit Buyer to hire third party external auditors to verify Supplier and third party compliance with their obligations under the Service Agreement and/or Order. Additionally, upon request, Supplier shall provide Buyer with any audit reports issued under ISO 27001, ISO 29100, SSAE 16 (or SAS 70), SSAE 18, SOC 2, OR ISAE 3402 that covers Buyer Personal Information;

2.1.7 will maintain reasonable and appropriate technical, physical, and administrative safeguards intended to protect Buyer Personal Information. These measures will include reasonable restrictions upon physical access to any locations containing Buyer Personal Information, such as the storage of such records in locked facilities, storage areas, or containers. Supplier must periodically re-

evaluate the measures adopted to ensure that they remain reasonable and appropriate;

2.1.8 provide Buyer with commercially reasonable assistance in: (i) deleting Buyer Personal Information in response to a request by an individual or legal representative; (ii) where relevant, enabling individuals to opt-out; and (iii) when Supplier is providing an electronic tool or software, distributing a privacy notice;

2.1.9 provide a privacy notice to individuals with whom the Supplier has direct contact unless Supplier and Buyer agree in writing that the privacy notice obligation is solely Buyer's responsibility;

2.1.10 pursuant to Buyer's written instructions, provide Buyer with the ability to purge Buyer Personal Information older than one year or such other time period agreed in writing upon in writing by the Parties, unless otherwise required to retain the data by applicable law; and

2.1.11 immediately advise Buyer in writing if it receives or learns of any: (i) complaint or allegation indicating a violation of Data Privacy Laws regarding Buyer Personal Information; (ii) request from one or more individuals seeking to access, correct, or delete Buyer Personal Information; (iii) inquiry or complaint from one or more individuals relating to the collection, Processing, use, or transfer of Buyer Personal Information; and (iv) regulatory request for, subpoena, search warrant, or other legal, regulatory, administrative, or governmental process seeking Buyer Personal Information (collectively, "Data Privacy Matters"). If Supplier learns of any Data Privacy Matters, Supplier shall provide assistance to Buyer, fully cooperate with Buyer in investigating the matter, including but not limited to, providing the relevant information to Buyer, preparing a response, implementing a remedy, and/or cooperating in the conduct of and defending against any claim, court or regulatory proceedings. Buyer shall be responsible for communicating with individuals regarding their Buyer Personal Information in connection with such Data Privacy Matters unless Buyer 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 Buyer Personal Information required to comply with applicable law. Unless prevented by applicable law, Supplier shall provide Buyer with advance written notice of any such Data Privacy Matters sufficient to allow Buyer to contest legal, regulatory, administrative, or other governmental processes.

2.2 Supplier shall provide written notice to Buyer 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 Buyer Personal Information of which it becomes aware (a “Security Breach”). If Supplier is unable to provide notice within 48 hours, Supplier shall provide Buyer with an explanation for the delay that Buyer will be entitled to share with regulators. Supplier shall take all reasonable measures to contain and remedy the Security Breach, wherever possible; provide Buyer 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 “Security Breach Notice”) without the prior written consent of and prior written approval by Buyer of the content, media and timing of the Security 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 Buyer prior to providing any Security Breach Notice. Where the Security Breach (i) involves data on the Supplier’s networks or systems or (ii) is the fault of the Supplier, then Supplier will, at the request of Buyer, 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.

2.3 In the event Supplier shall provide to Buyer 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.

2.4 All Buyer Personal Information acquired by Supplier shall be returned or destroyed (at Buyer’s option), unless and to the extent that: (i) such Buyer Personal Information 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 Buyer Personal Information after termination or completion of the Order after waiting 30 days to allow Buyer to request return of Buyer Personal Information.

2.5 If the Service Agreement and/or Order involves collection or Processing of Buyer 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, Buyer Personal Information.

2.6 If the Service Agreement and/or Order involves the provision of Services where the Supplier will (i) act as a Controller (as that term is defined in the EU Directive) and (ii) transfer Buyer Personal Information from any country in the European Economic Area or Switzerland (collectively, “EEA/CH”) to outside the EEA/CH, then the Buyer and Supplier agree that the terms of the Model Contract Clauses (also called the Standard Contractual Clauses) adopted by the European Commission in Decision 2004/915/EC (hereinafter the “Controller Model Clauses” or the “Model Clauses”) are incorporated by reference as if set forth herein. If the Service Agreement and/or Order involves the cross-border transfer of Buyer Personal Information from any country in the EEA/CH to outside the EEA/CH but the Supplier will not act as a Controller, then the Buyer and Supplier agree that the terms of the Model Contract Clauses (also called the Standard Contractual Clauses) adopted by the European Commission in Decision 2010/87/EU (hereinafter the “Processor Model Clauses” or the “Model Clauses”) are incorporated by reference as if set forth herein. Notwithstanding the foregoing, Buyer and Supplier agree that:

2.6.1 The Model Clauses may be reformatted as a stand-alone document with the signatures to the Service Agreement and/or Order or the Parties will execute the Model Clauses as a separate stand-alone document. The stand-alone Model Clauses may be filed with regulators and/or used for any other legally permissible purpose and have the effect as if signed directly.

2.6.2 If either Party seeks to register the Model Clauses with a regulator, and the regulator rejects the registration, the Parties shall work together to modify the exhibits to the Model Clauses to address the regulator’s requirements.

2.6.3 If any of the terms of the Model Clauses conflict with any terms of the Service Agreement and/or Order, the Model Clauses shall prevail.

2.6.4 If Supplier engages any subcontractors that will access Buyer Personal Information covered by the Model Clauses, the Supplier shall ensure that

transfers to the subcontractor comply with the Model Clauses.