Supplement for the Security of Personal Data

Seller agrees that it shall comply with the following provisions with respect to all "Personal Information" collected, used, transmitted or maintained for The Boeing Company. This Addendum stipulates privacy, confidentiality, and security requirements and demonstrates compliance with applicable privacy, security and data protection laws.

1. Definitions

(a) "Agreement Personal Data" means the Personal Information (described in Annex 1 or the Statement of Work) processed by the Seller on behalf of Boeing pursuant to this Agreement.

(b) "Boeing Group" means: (i) [NAME OF GROUP COMPANY TO BE INCLUDED]; (ii) [NAME OF GROUP COMPANY TO BE INCLUDED, ETC.] and (iii) [Boeing's holding company and ultimate holding company and each of its subsidiary companies and its holding company and ultimate holding company's subsidiary companies from time to time] (with "holding company" and "subsidiary" having the meanings given to them in section 1159 of the Companies Act 2006), each shall be a "Boeing Group Company".

(c) "European Personal Data" means any Personal Data Processed by Boeing or any Boeing Group Company as a Data Controller either (i) located within the European Union (EU) or the European Economic Area (EEA) or (ii) where such Personal Data is otherwise processed by that Data Controller subject to the GDPR.

(d) "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation.

(e) "Internal Control Report" means a Type II Service Organizational Control (SOC) report (based on the SSAE 16 or ISAE 3402 model), any successor report thereto, or other mutually acceptable standard accepted by both parties in writing.

(f) "Personal Information" means European Personal Data and any and all data (regardless of format) that on its face or in combination with other information (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifiers set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location.

(g) "Privacy Laws" means all applicable U.S. (federal and state) laws, other countries' national and local laws, and international laws that regulate the Processing of Personal Information. Applicable Privacy Laws may include State, National, and other applicable laws that specify data protection, privacy, security or security breach notification obligations that affect the Agreement Personal Data or the provision of the services by Seller. In respect of European Personal Data this shall include decisions and guidance by relevant supervisory authorities relating to data protection, the Processing of Personal Data and privacy, including:

(i) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the Processing of Personal Data;

(ii) local implementing legislation within the European Union in respect of (i) above, for example the Data Protection Act 1998 in the UK;

(iii) (with effect from 25 May 2018) the GDPR;

(iv) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the protection of privacy in the electronic communications sector;

(v) local implementing legislation within the European Union in respect of (iv) above, for example the Privacy and Electronic Communications (EC Directive) Regulations 2003 in the UK (as may be amended by the proposed EU Regulation on Privacy and Electronic Communications); and

(vi) any legislation that, in respect of the territories covered by this Agreement, replaces or converts into domestic law the GDPR, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, including in respect of the Processing of Personal Data and privacy as a consequence of the United Kingdom leaving the European Union;

and references to **"Data Controller" "Data Processor", "Data Subjects"**, **"Personal Data"**, **"Process"**, **"Processed"** and **"Processing"** have the meanings set out in, and will be interpreted in accordingly by such applicable laws.

(h) "Data Breach" means a "Personal Data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law), any other actual, suspected or threatened compromise or disclosure of Agreement Personal Data or the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, European Personal Data transmitted, stored or otherwise Processed under this Agreement.

(i) "Sensitive Personal Information" includes: (i) all government-issued identification numbers (such as Social Security number or driver's license number), (ii) all financial account numbers (including payment card information and health insurance numbers), (iii) individual medical records, genetic and biometric information, (iv) all data obtained from a U.S. consumer reporting agency (such as employee background investigation reports, credit reports, and credit scores), (v) user account credentials, such as usernames, passwords, security questions/answers and other password recovery data, and, in respect of European Personal Data also has the meaning set out in, and will be interpreted in accordance with:

(i) in respect of Processing undertaken on or before 24 May 2018, the definition of "Sensitive Personal Data" in the Data Protection Act 1998;

(ii) in respect of Processing undertaken on or after 25 May 2018, the types of Personal Data described in Article 9(1) of the GDPR; and

(iii) in respect of Processing undertaken on or after the date on which legislation comes into force that replaces or converts into domestic law the GDPR, the description of Personal Data that is most similar to those set out within this definition, in that legislation.

(j) "Services" means any and all services that Boeing requests the Seller to perform under this agreement or any other contract, Statement of Work or agreement that involves Processing of Personal Information and/or Agreement Personal Data.

(k) "Subprocessor" means any third party appointed by the Seller in accordance with this Agreement (including an affiliate of Seller) to Process Agreement Personal Data and/or that provides any services to Seller and that may have access (including inadvertent access) to any Agreement Personal Data. For purposes of the Agreement, Subprocessor may be referred to as supplier or subcontractor.

(l) "Transfer" means to disclose or otherwise make the Personal Information and/or Agreement Personal Data available to a third party (including to any affiliate or Subprocessor of Seller), either by physical movement of the Personal Information and/or Agreement Personal Data to such third party or by enabling access to the Personal Information and/or Agreement Personal Data by other means.

(m) "Valid Transfer Mechanism" means any data transfer mechanism recognized by the appropriate legal entities as a legitimate basis for the international transfer of Personal Information. This includes any methods recognized by the EU Commission for providing "adequate safeguards" in respect of international transfers of Personal Information outside of the EEA.

Wherever under this Agreement Boeing's consent is required before the Seller is permitted to do a particular act or thing, unless otherwise expressly provided, Boeing is entitled to give or withhold consent or make consent subject to conditions at its sole discretion.

References to Boeing in this [Schedule/Agreement] shall be read as the relevant Boeing entity which is the Data Controller of the relevant Agreement Personal Data and/or the Services provided in respect of such Agreement Personal Data by the Seller. Each such entity shall be able to enforce the terms of this [Schedule/Agreement] directly against the Seller in respect of those Services.

2. General Obligations

(a) Seller shall only Process or Transfer Agreement Personal Data for the purposes of performing and to the extent required to provide the Services under this Agreement or as specifically authorized by Boeing. Agreement Personal Data shall not be used for any other purpose.

(b) Boeing authorises the Seller to Process the Agreement Personal Data during the [Term]/[term of this Schedule/Agreement] as a Data Processor solely for the purpose of providing the Services

(c) Seller shall promptly inform Boeing in writing: (i) if it cannot comply with any material term of its agreement with Boeing regarding the Services (if this occurs, Seller shall use reasonable efforts to remedy the non-compliance, and Boeing shall be entitled to terminate Seller's further Processing of the Agreement Personal Data); (ii) of any request for access to any Agreement Personal Data received from an individual who is (or claims to be) the subject of the data; (iii) of

any request for access to any Agreement Personal Data received by Seller from any government official (including any data protection agency or law enforcement agency) unless it is explicitly prohibited by law from notifying Boeing of the request; (iv) of any other requests with respect to Agreement Personal Data received from Boeing employees or other third parties, other than those set forth in the agreement. Seller understands that it is not authorized to respond to these requests, unless explicitly authorized by Boeing or the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Seller.

(d) Each party must stay informed of the legal and regulatory requirements for its Processing of Agreement Personal Data.

(e) Seller represents and warrants that it shall, at all times, fully comply with Privacy Laws that are applicable to the Processing, as well as Seller's own privacy notices.

(f) Seller has provided Boeing with responses to Boeing information requests along with other information as needed to support those responses. Seller represents and warrants that all such responses and information were accurate, current and complete, in all material respects.

(g) Once per year, Seller shall provide Boeing with copies of applicable Internal Control Reports. Boeing understands that the responses and Internal Control Reports contain Confidential Information of the Seller, and it shall not disclose the Internal Controls Reports other than to its auditors and advisors in connection with verifying Seller's compliance with this agreement or Boeing security and privacy program requirements. In addition to Internal Control Reports, Seller will provide Boeing with responses to targeted questions pertinent to determining the security of Agreement Personal Data in a timely, complete, and accurate manner.

(h) If the Services involve the collection of Agreement Personal Data directly from individuals, Seller will provide the individuals with a clear and conspicuous privacy notice, which notice shall either (i) be Boeing's privacy notice, or (ii) be Seller's privacy notice, provided that such notice must address any legal requirements for such notices in the jurisdictions where it is given, be translated into the languages used in connection with Seller's interaction with the individuals, and indicate that Seller is Processing the data as a processor on behalf of its clients. All such notices must be approved by Boeing in advance of their distribution.

(i) If the Personal Information will include "protected health information" (or "PHI") as defined in the HIPAA Privacy and Security Rules, Seller and Boeing shall execute an appropriate Business Associate Agreement as required by HIPAA.

(j) Seller shall ensure adequate protection for Agreement Personal Data.

(k) Seller shall reasonably cooperate with Boeing and with its affiliates, members of the Boeing Group and representatives in responding to inquiries, incidents, claims and complaints regarding the Processing of the Agreement Personal Data or as otherwise needed for Boeing to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws.

(l) Seller shall retain Agreement Personal Data no longer than is necessary for the purposes for which it was provided, unless otherwise compelled by law.

(m) Seller will notify Boeing without undue delay if, in the performance of the Services, it identifies any areas of actual or potential non-compliance with the Data Protection Laws or this [Agreement/Data Processing Addendum].

(n) Seller will not, without the express prior written consent of Boeing or the relevant member of the Boeing Group:

(i) convert any Agreement Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data;

(ii) use any Agreement Personal Data for automated decision making, profiling, or other analytics purposes;

(iii) match or compare any Agreement Personal Data with or against any other Personal Data (whether Seller's or any third party's); or

(iv) procure a Subprocessor to perform any of these tasks.

(o) Seller shall assist Boeing in:

(i) responding to requests for exercising Data Subjects' rights under the Data Protection Laws, including by appropriate technical and organisational measures, insofar as this is possible;

(ii) documenting any Data Breach and reporting any Data Breach to any supervisory authority and/or Data Subjects;

(iii) taking measures to address Data Breaches, including, where appropriate, measures to mitigate their possible adverse effects; and

(iv) conducting privacy or data protection impact assessments of any Processing operations and consulting with supervisory authorities, Data Subjects and their representatives accordingly.

3. <u>Confidentiality and Data Access</u>

(a) Personal Information of Boeing Affiliated Personnel (employees, dependents, etc.,) is considered Confidential Information of Boeing, and Seller must maintain all such Personal Information and Agreement Personal Data in strict confidence. This confidentiality applies regardless of whether the information was provided directly from Boeing, directly from the data subject, gathered in open source, or provided to or from Seller on Boeing's behalf. Seller may disclose Agreement Personal Data to its employees/personnel only when such individuals have a need to know, and require access to the Agreement Personal Data to perform the Services of this Agreement.

(b) Prior to allowing any employee or contingent worker to Process any Agreement Personal Data, Seller shall (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement (in a form acceptable to the Boeing), (iii) provide the individual with appropriate privacy and security training, (iv) require the individual to comply with this [Schedule/Agreement], and (v) ensure the individual is appropriately reliable, qualified and trained in relation to their Processing of Agreement Personal Data. Seller will also monitor its employees and contingent workers for compliance with the privacy and security program requirements.

4. <u>Approvals for Transfers and Subprocessors</u>

(a) Seller will not engage or use any third party for the Processing of Agreement Personal Data or permit any third party to Process Agreement Personal Data without the prior written consent of Boeing.

(i) If Seller appoints a Subprocessor pursuant to clause 4(a) which involves the Processing of European Personal Data, Seller shall demonstrate to Boeing that there is in place a written contract between Seller and the Subprocessor that specifies the Subprocessor's Processing activities and imposes on the Subprocessor the same terms as those imposed on Seller in this [Schedule/Agreement].

(b) Seller will remain responsible and liable to Boeing and the other members of the Boeing Group for all acts and omissions of Subprocessors as if they were its own.

(c) Seller shall not Transfer Agreement Personal Data to any Subprocessors or other third parties unless such Processing is required to perform the Services. Seller shall provide Boeing with a list of all such Subprocessors.

(d) Subject to clause 4(e), Seller shall not Transfer the Agreement Personal Data across any national borders, nor permit Processing of or remote access to the Agreement Personal Data by any employee, contingent worker, affiliate, Subprocessor or other third party across national borders (or in the case of European Personal Data outside the EEA) unless Seller has the prior written consent of Boeing for such transfer, and has verified that such transfer complies with all applicable laws (including all applicable Privacy Laws) and Valid Transfer Mechanisms.

(e) With regard to Transfers of European Personal Data, the parties shall assure adequate protection for the European Personal Data as follows:

_____ The Seller shall enter into approved EU Standard Contractual Clauses (Processors), a copy of which is attached hereto.

_____ The Seller has certified its compliance to the EU-US Privacy Shield Program. Seller shall maintain its certification to the Privacy Shield for so long as it processes any European Personal Data. In the event that EU authorities or courts determine that the Privacy Shield is not an appropriate basis for transfers, Seller shall promptly execute an approved EU Standard Contractual Clauses (Processors), which shall be incorporated herein upon execution.

_____ The Seller shall Transfer European Personal Data pursuant to its approved set of Binding Corporate Rules for Data Processors.

In the event that EU authorities or courts determine that the Transfer mechanism selected above is no longer an appropriate basis for Transfers, Seller and Boeing shall promptly take all steps reasonably necessary to demonstrate adequate protection for the European Personal Data, using another approved mechanism. Seller understands and agrees that Boeing may terminate the Transfers as needed to comply with the EU Data Protection Laws.

5. Information Security Requirements

(a) Seller shall have implemented (and will provide reasonable assistance to Boeing and the other members of the Boeing Group to implement) and shall have documented appropriate administrative, technical, organisational and physical measures to protect Agreement Personal Data against accidental or unlawful destruction, alteration, compromise, or unlawful disclosure or access, and ensure a level of security appropriate to the risk presented by Processing the Agreement Personal Data, in particular from a Data Breach. Seller will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Seller will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Agreement Personal Data, and ensure that these risks are addressed.

(b) Seller shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services (including restoring access to the Agreement Personal Data) in a timely manner after a disruptive event. Seller will regularly test and monitor the effectiveness of its business continuity and disaster recovery plans. At appropriate intervals or as otherwise requested by Boeing, Seller will provide a copy of its written business continuity and disaster recovery plans to Boeing.

(c) If the Processing involves the transmission of Agreement Personal Data over a network, Seller shall have implemented appropriate supplementary measures to protect the Agreement Personal Data against the specific risks presented by the Processing. Personal Information may not be transmitted over any network unless it has been appropriately protected, such as with encryption.

(d) Personal Information and any European Personal Data may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks, USB or flash drives, personal digital assistants (PDAs) or mobile phones, DVDs, CDs or computer tapes) unless it is encrypted. Any employees of Seller who handle Sensitive Personal Information are required to follow a clean desk policy by clearing their desk of all papers with Sensitive Personal Information when they leave their desk at any time during the day or at the end of the day.

(e) Upon request, Seller shall provide Boeing with information about the Seller's information security program. Notwithstanding the provisions in clause 5(f), Seller shall also submit its data processing facilities for audit, which shall be carried out by Boeing (or by an independent auditor designated by Boeing) in a mutually-agreeable manner no more than ten (10) days after any

such request. Seller shall reasonably cooperate with any such audit. In the event that any such audit reveals material gaps or weaknesses in Seller's security program, Boeing shall be entitled to terminate Seller's Processing of Agreement Personal Data until such issues are resolved. Seller shall also cooperate with any audits conducted by any regulatory agency that has authority over Boeing's needed to comply with applicable law.

(f) In respect of any European Personal Data Seller will, and will procure that Subprocessors will:

(i) make available to Boeing and the other members of the Boeing Group all information necessary to demonstrate compliance with the obligations set out in this [Schedule/Agreement]; and

(ii) allow for and contribute to audits, including inspections, conducted by Boeing or another auditor mandated by Boeing.

(g) In respect of European Personal Data, Seller will prepare and securely maintain a record of all categories of Processing activities carried out on behalf of Boeing and other members of the Boeing Group in relation to the Agreement Personal Data, including as a minimum: (i) its name and contact details and details of its Data Protection officer or other person with responsibility for Data Protection compliance; (ii) the categories of Processing it carries out on behalf of Boeing and other members of the Boeing Group; (iii) any transfers of Agreement Personal Data outside the European Economic Area (as it is made up from time to time) and/or international organisations; (iv) a general description of the technical and organisational security measures referred to in clause 5(a); and (v) the same information in relation to any Subprocessor, together with its name and contact details (together the "**Data Record**"). Seller will promptly upon request securely supply a copy of the Data Record to Boeing.

(h) Seller will promptly and thoroughly investigate all actual, potential, or suspicions of unauthorized access to, use or disclosure of Agreement Personal Data and of Data Breaches of systems containing, transmitting or otherwise Processing Agreement Personal Data.

(i) Seller will notify Boeing without undue delay (and in any event no later than 24 hours) upon becoming aware of any reasonably suspected, "near miss" or actual Data Breach, including the nature of the Data Breach, the categories and approximate number of Data Subjects and Agreement Personal Data records concerned and any measure proposed to be taken to address the Data Breach and to mitigate its possible adverse effects. Seller shall provide Boeing with all information about the Data Breach reasonably needed by Boeing to assess its incident response obligations. Where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay, but Seller (and Subprocessors) may not delay notification under this clause 5(i) on the basis that an investigation is incomplete or ongoing. Seller will not, and will procure that Subprocessors will not, make or permit any announcement in respect of the Data Breach to any person without Boeing's prior written consent. Seller shall bear all costs associated with resolving a Data Breach, including (without limitation), conducting an investigation, engaging appropriate forensic analysis, notifying individuals, relevant government entities and others as required to by law or the Payment Card Industry Data Security Standard, providing individuals with credit monitoring (or other appropriate remediation service), and responding to individual, regulator and media inquiries.

(j) When the Seller ceases to perform Services for Boeing (and at any other time, upon request), Seller will promptly either, at the option of Boeing, (i) securely return all Agreement Personal Data (and all media containing copies of the Agreement Personal Data) to Boeing, or (ii) securely purge, delete and destroy the Agreement Personal Data and securely delete any remaining copies and promptly certify (via a director or officer) when this exercise has been completed. In the event that Agreement Personal Data cannot be returned, the controls stipulated in this Agreement will remain in effect until such data can be destroyed. Electronic media containing Agreement Personal Data will be disposed of in a manner that renders the Agreement Personal Data unrecoverable. Seller will provide Boeing with an Officer's Certificate to certify its compliance with this provision. If Seller is required by applicable law to retain any Agreement Personal Data, Seller warrants that it shall (i) ensure the continued confidentiality and security of the Agreement Personal Data, (ii) securely delete or destroy the Agreement Personal Data when the legal retention period has expired, and (iii) not actively Process the Agreement Personal Data other than as needed for to comply with law.

6. Insurance

Seller shall carry appropriate insurance, including but not limited to Professional and Technology E&O policies including Network Security and Privacy Liability coverage, from insurance companies holding minimum AM Best ratings of A- (VII) or higher, in amounts not less than US $5,000,000.00 per claim, to address the risks from its Processing of the Agreement Personal Data, including risks of cyber-attacks and security breaches. Any retroactive date on such required policy must be no later than the date of execution of this Agreement. The carrying of the above-described coverage shall in no way to be interpreted as relieving or increasing the responsibility or liabilities of either party under this Agreement or any applicable law, statute, regulation or order.

7. Indemnification

Seller agrees to indemnify, defend and hold harmless Boeing, each member of the Boeing Group, its affiliates, and their respective officers, directors, members, shareholders, agents, employees, representatives, assigns and successors from, and on demand reimburse Boeing (or one or more members of the Boeing Group as appropriate) for any and all damages, losses and/or expenses (including attorneys' fees and other costs of defense) incurred in connection with any and all demands, suits, claims, investigations, fines (including monetary penalty notices) and liabilities whatsoever arising from: (1) Seller's violation of applicable law and/or regulation and (2) Seller's breach of any of the representations, warranties or obligations under this Agreement (including any related act or omission by Seller).

8. Breach

A breach of this Data Protection Addendum by Seller or any Subprocessor will be a material breach of this Agreement.