Airship Partner Data Protection Addendum

This Data Protection Addendum (“DPA”) is incorporated into and made a part of that certain partnership agreement between Airship, Group, Inc. ("Airship") and _____ ("Partner"), (each a “Party” and together the “Parties”), dated _____ (the "Partner Agreement") and governs the data sharing between Airship and Partner.

With respect to provisions regarding Processing of Personal Data, in the event of a conflict between this DPA and any other provision of the Agreement between Airship and Partner, this DPA will control.

The purpose of this DPA is to establish a framework to address scenarios where:

1. Airship and Partner may, in connection with the Agreement, each be Controllers (as defined below) of Personal Data and, in certain cases, transfer that Personal Data to the other party for that other party to act as a Controller of that Personal Data;
2. Airship and Partner may each be Controllers of Personal Data and, in certain cases, transfer that Personal Data to the other party for that other party to provide certain services to the other party as a Processor; or
3. Airship and Partner may each be a Processor of a Joint Customer’s Personal Data and transfer such data to the other party for processing at the direction of that Joint Customer.

1. Definitions

All terms which are capitalized in this DPA will have the meanings set forth below, or, if not defined in this DPA, will have the meanings assigned to those terms in the Partner Agreement.

1.1. “**Airship Personal Data**” means any Personal Data for which Airship acts as a Controller.

1.2. “**Airship Security Measures**” means the technical and organizational security measures implemented by Airship for the Processing of Personal Data in the Airship Services, as described at https://www.airship.com/legal/security-measures/ (or such successor URL as Airship may designate from time to time) and as further detailed in Annex II to this DPA.

1.3. “**Business**” and “**Service Provider**” shall have the meanings given to them in the CCPA.

1.4. “**California Personal Information**” means Personal Data that is subject to the protection of the CCPA.

1.5. “**Data Protection Laws**” means (i) EU Data Protection Laws; (ii) the data protection or privacy laws of the United States of America, including without limitation, the California Consumer Privacy Act of 2018, (“CCPA”), as amended

by the California Privacy Rights Act of 2020 ("CPRA") and its implementing regulations, (together the "CCPA"), state Health Privacy Laws, and other comprehensive state privacy laws as may be applicable; (iii) the data protection or privacy laws of the United Kingdom, ("UK Data Protection Laws"); or (iv) the similar laws of any other country, as applicable.

1.6. **"EU Data Protection Laws**" means data protection laws applicable in Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation), as may be amended from time to time ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (the "ePrivacy Directive" as may be amended, superseded or replaced).

1.7. **"Health Privacy Laws**" means U.S. state laws and regulations governing the privacy, security, and processing of consumer health data collected through applications, websites, or other digital services, including but not limited to the California Confidentiality of Medical Information Act, the Washington My Health My Data Act, and similar state legislation that regulates health information outside of the healthcare context. For clarity, "Health Privacy Laws" specifically excludes the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA").

1.8. "**EU Personal Data**" means Personal Data the sharing of which pursuant to this DPA is regulated by EU Data Protection Laws.

1.9. "**Joint Customer**" means a customer of both Partner and Airship who has requested access to an integration made available by either Partner or Airship, as applicable.

1.10. "**Joint Customer Personal Data**" means any Personal Data for which a Joint Customer acts as a Controller."**Partner Personal Data**" means any Personal Data for which Partner acts as a Controller.

1.11. "**Partner Security Measures**" means the technical and organizational security measures implemented by Partner for the Processing of Personal Data, which shall be equivalent to or exceed the standards described in Annex II to this DPA and as further detailed by Partner in Annex II.

1.12. "**Personal Data"** has the same meaning as the term "personal data" or "personal information" under the applicable Data Protection Laws where such information is contained within Airship Personal Data, Partner Personal Data, or Joint Customer Personal Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.

1.13. **"Request**" means a written request from a Data Subject to exercise one or more data subject rights provided for under Data Protection Laws in respect of Personal Data processed under this DPA.

1.14. "**Process**" or "**Processing**" means means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by

automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.15. "**Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

1.16. "**SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (also referred to as the "New SCCs").

1.17. "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data.

1.18. "**Service**" means the Airship Services described in the Documentation and procured by the applicable party, and any other services provided by Airship or Partner as described under the Partner Agreement or Joint Customer Agreement, as applicable.**"Transfer Mechanism"** means an onward transfer mechanism, to the extent the Processing of Personal Data under this DPA requires the lawful transfer of Personal Data from a jurisdiction (i.e., the European Economic Area, the United Kingdom, Switzerland, or any other jurisdiction listed in this DPA) to a party located outside of that jurisdiction. The terms set forth in Section 7 (Cross Border Transfers) of this DPA will apply to such Transfer Mechanism.

1.19. "**Sub-processor**" means any entity that provides processing services to a Data Processor.

1.20. **"UK Addendum**" means the International Data Transfer Addendum issued by the United Kingdom's Information Commissioner's Office ("ICO") to the EU Commission's Standard Contractual Clauses VERSION B1.0, in force 21 March 2022.The terms "**Controller**", "**Data Subject**", "**Data Importer**","**Data Exporte**r", **Member State**", and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

1.21. The terms "**Business**", "**Personal Information**", "**Partner**", "**Sale**," and "**Sell**" are as defined in Section 1798.140 of the CCPA.

1.22. All other capitalized terms not defined in this DPA shall have the meanings set forth in the Partner Agreement.

2. General Requirements

2.1. In relation to the Processing of any Personal Data under or in relation to the Partnership Agreement, each Party shall comply with its respective obligations as either a Controller or Processor as applicable under the Data Protection Laws and any other relevant applicable Data Protection Laws. In particular, and without limitation to the generality of the foregoing, the Party that discloses Personal Data (the "**Disclosing Party**") to the other party (the "**Receiving Party**") shall: (a) ensure that it has a lawful basis, as required by the applicable Data Protection

Laws, for any transfer of Personal Data to the Receiving Party for the Processing activities contemplated by this DPA; (b) upon request from the Receiving Party, produce proof of the lawful basis referred to in this clause; (c) take reasonable measures to ensure that the Personal Data transferred to the Receiving Party is accurate and up-to-date to the extent such Personal Data is under the control of the Disclosing Party; (d) where the Disclosing Party is a Controller or as otherwise instructed by the Controller, ensure that it has provided Data Subjects whose Personal Data is being transferred to the Receiving Party with appropriate notice of the transfer and subsequent Processing by the Receiving Party, as required by the Data Protection Legislation; and (e) where the Disclosing Party is a Controller or as otherwise instructed by the Controller, ensure that it is not transferring any Personal Data of a Data Subject who has withdrawn consent or objected to the Processing of their Personal Data by the Disclosing Party and/or the Receiving Party.

2.2. **Prohibited Data.** Unless otherwise specifically agreed in writing, neither Party shall Process via the Services provided under this DPA any government-issued ID numbers such as passport numbers, individual medical or health information (except as permitted under applicable Health Privacy Laws with appropriate safeguards), individual financial information or account numbers (including without limitation, credit or debit card numbers or bank account numbers), or "special categories of personal data" under the EU Data Protection Laws or similar sensitive information under other comparable laws or regulations (collectively, "Prohibited Data"). Each Party shall have sole responsibility for: (a) the accuracy and quality of Personal Data it Processes; (b) obtaining the appropriate permissions for legally Processing and using the Personal Data; and (c) the means by which it acquires and uses Personal Data as contemplated under this DPA. Where a Party's Processing is subject to Health Privacy Laws, that Party is responsible for determining whether any Personal Data it Processes constitutes health data under applicable Health Privacy Laws and for ensuring its own compliance with such Health Privacy Laws.

2.3. **Joint Processor Scenarios**

2.3.1. Each Party, to the extent that it, along with the other Party, acts as a Processor with respect to Joint Customer Personal Data, will (a) comply with the instructions and restrictions set forth in any agreement(s) with the Joint Customer, ("Joint Customer Agreement"), and (b) reasonably cooperate with the other Party to enable the exercise of data protection rights as set forth in the applicable Data Protection Laws or as otherwise requested by the Data Controller. The Parties both acknowledge and agree that each Party is acting as a Processor for the Joint Customer and neither party is engaging the other as a Sub-processor.

2.4. **Controller-to-Controller Scenarios**

2.4.1. Each Party, to the extent that it acts as a Controller with respect to Personal Data, will reasonably cooperate with the other Party to enable the exercise of data protection rights as set forth in applicable Data

Protection Laws. The Parties acknowledge that each is Processing Personal Data as separate and independent Controllers, and are not joint controllers as defined in the applicable Data Protection Laws.

2.5. Controller-to-Processor Scenarios

2.5.1. Relationship of the Parties. The rights, responsibilities, and obligations of the parties with respect to Sections 3-6 of this DPA shall be as follows: For Processing operations where Airship Processes Personal Data on Partner's behalf and at Partner's direction, the term "Processor" refers to Airship, the term "Controller" refers to Partner, and the term "Personal Data" refers to Partner Personal Data. For data Processing operations where Partner Processes Personal Data on Airship's behalf and at Airship's direction, the term "Processor" refers to Partner, the term "Controller" refers to Airship, and the term "Personal Data" refers to Airship Personal Data.

2.5.2. Scope of Processing. In the context of the scenarios described in Section 2.5.1 above, each Party agrees to Process Personal Data only for the purposes set forth in the applicable Partner Agreement and/or the Partner's agreement(s) with the Joint Customer Agreement, as applicable. The categories of Personal Data Processed and the categories of Data Subjects are described in Schedule A to this DPA. The specific categories of Personal Data Processed will vary according to the Services package and the specific functionalities utilized, and will depend on implementation choices, the features and functionalities activated, and data collection practices. For the avoidance of doubt:

2.5.2.1. Instructions by the Controller to the Processor to Process Personal Data include: (a) Processing in accordance with the applicable Agreement and Order Form(s); (b) Processing initiated by authorized users in their use of the Service; (c) Processing to comply with other reasonable instructions provided by the Controller (e.g., via email) where such instructions are consistent with the terms of the applicable Agreement; and (d) Processing in accordance with all configuration of the Service by or for the Controller.

2.5.2.2. The Processor shall, as soon as reasonably practicable upon receiving any instruction that, in the Processor's opinion, infringes applicable Data Protection Laws, inform the Controller of such concern.

3. Controller Obligations

3.1. Both parties, in their capacity as a Controller, agree:

3.1.1. To Process any Personal Data which it obtains or holds under or in relation to the Partner Agreement only for the purposes of carrying out its obligations under the Partner Agreement;

3.1.2. To take appropriate technical and organizational measures against unauthorized or unlawful Processing of personal data and against

accidental loss or destruction of or damage to personal data, including without limitation a Security Breach; and

3.1.3. To ensure that any recipient of the other party's Personal Data is subject to written contractual obligations concerning the Personal Data, as required by the Data Protection Laws;

3.1.4. To ensure that, for any transfers of Personal Data in the context of the Services, the Personal Data will be protected with the same level of protection as provided by this DPA and it will implement any data transfer mechanism as required under the Data Protection Laws. Both parties agree not transfer any of the other party's Personal Data outside the European Economic Area or the United Kingdom unless it first: (a) notifies the other Party in advance of the transfer; (b) ensures that the transfer of Personal Data subject to the EU Data Protection Laws is made subject to the terms of Section 7 of this DPA (c) ensures that the transfer of Personal Data subject to the UK Data Protection Laws is made subject to the terms of Section 7 of this DPA; or (d) ensures that the transfer is made in compliance with Articles 45 to 47, inclusive, of the GDPR or equivalent applicable provisions of the Data Protection Laws;

3.1.5. To promptly notify the other Party if a Data Subject whose Personal Data is Processed in connection with this DPA withdraws his or her consent to such Processing;

3.1.6. To promptly notify the other Party about the receipt of any Data Subject access request from a Data Subject whose Personal Data is Processed in connection with the performance of each Party's respective obligations under the Partner Agreement and this DPA, and to provide the other Party with reasonable assistance in complying with any such data subject access request, but not to disclose or release any Personal Data without first consulting the other Party wherever possible. The Parties agree that the responsibility for complying with a Data Subject's rights request belongs to the Party receiving such a request in respect of the Personal Data held by that Party. However, the Parties shall provide each other reasonable assistance, as is necessary, to enable each Party to comply with their obligations to respond to Data Subjects' requests to exercise their rights and to respond to any other queries or complaints from Data Subjects. The Parties shall, as is necessary, keep each other informed about such disputes and, where appropriate, reasonably cooperate in resolving them; and

3.1.7. To notify the other Party promptly and without undue delay, but in no event later than forty-eight (48) hours after becoming aware, of any Security Breach concerning Personal Data Processed in connection with the Partner Agreement. Such notifications as to Airship shall be sent to security@airship.com and as to Partner to _____.

4. Processor Obligations

4.1. Processing Requirements

4.1.1. Both parties, in their capacity as a Processor, agree:

4.1.1.1. To Process Personal Data (a) only for the purpose of providing the Processor's product and services using appropriate technical and organizational security measures; and (b) in compliance with the instructions received from the Controller. The Processor will not use or Process Personal Data for any other purpose. The Processor will promptly inform the Controller in writing if it cannot comply with the requirements under this DPA, in which case the Controller may terminate the DPA, and any applicable Partner Agreement, or take any other reasonable action, including suspending data Processing operations;

4.1.1.2. To inform the Controller promptly and without undue delay if, in the Processor's opinion, an instruction from the Controller violates applicable Data Protection Laws;

4.1.1.3. To take commercially reasonable steps to ensure that (a) persons employed by it and (b) other persons engaged to perform on the Processor's behalf comply with the terms of this DPA and applicable Partner Agreements;

4.1.1.4. That it represents and warrants that its employees, authorized agents and any Sub-processors are subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to Process the personal data who is not under such a duty of confidentiality;

4.1.1.5. That if it intends to engage Sub-processors to help it satisfy its obligations in accordance with this DPA or to delegate all or part of the Processing activities to such Sub-processors, (a) provide a list of Sub-processors currently engaged by the Processor to the Controller and notify the Controller of the engagement of any new Sub-processors at least 30 days in advance, giving the Controller the opportunity to object; (b) remain liable to the Controller for the Sub-processors' acts and omissions with regard to data protection where such Sub-processors act on the Processor's instructions; and (c) enter into contractual arrangements with such Sub-processors binding them to provide the same level of data protection and information security to that provided for herein;

4.1.1.6. That upon request, provide the Controller with the Processor's privacy and security policies; and

4.1.1.7. To inform the Controller if the Processor undertakes an independent security review.

4.1.1.8. To comply with its obligations under any Joint Customer Agreement, and also notify the Joint Processor promptly and without undue delay, but in no event later than forty-eight (48) hours after becoming aware, of any Security Breach concerning Personal Data Processed in connection with the Joint Customer

Agreement. Such notifications as to Airship shall be sent to security@airship.com and as to Partner to _____.

4.1.1.9. To maintain appropriate technical and organizational security measures as set forth in Annex II to this DPA. When Airship acts as Processor, Airship shall implement and maintain the Airship Security Measures. When Partner acts as Processor, Partner shall implement and maintain the Partner Security Measures, which must be equivalent to or exceed the standards set forth in Annex II. Upon reasonable request from the Controller, the Processor shall provide evidence of compliance with its security obligations, including by making available summaries of relevant third-party certifications or attestations.

4.2. Notice to Controller

4.2.1. The Processor will immediately and without undue delay inform the Controller if the Processor becomes aware of:

4.2.1.1. Any non-compliance by Processor or its employees with this DPA or applicable Data Protection Laws relating to the protection of Personal Data Processed under this DPA;

4.2.1.2. Any legally binding request for disclosure of Personal Data by a law enforcement or government authority, unless the Processor is otherwise forbidden by law to inform the Controller, for example to preserve the confidentiality of an investigation by law enforcement authorities;

4.2.1.3. Any notice, inquiry or investigation by a Supervisory Authority with respect to Personal Data; or

4.2.1.4. Any complaint or request (in particular, requests for access to, rectification/ correction, objection, erasure, blocking or data portability of Personal Data) received directly from Data Subjects of the Controller. The Processor will not respond to any such request without the Controller's prior written authorization.

4.3. Assistance to the Controller

4.3.1. The Processor will provide timely and reasonable assistance to the Controller or to the Joint Processor to the extent requested by the Controller regarding:

4.3.1.1. Responding to any request from a Data Subject to exercise rights under applicable Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable);

4.3.1.2. The investigation of Security Breaches and the notification to the Supervisory Authority and the Controller Data Subjects regarding such Personal Data Breaches; and

4.3.1.3. where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

4.4. Required Processing

4.4.1. If the Processor is required by Data Protection Laws to Process any Personal Data for a reason other than in connection with the Partner Agreement, the Processor will inform the Controller of this requirement in advance of any processing, unless the Processor is legally prohibited from informing the Controller of such Processing (e.g., as a result of secrecy requirements that may exist under applicable EU member state laws).

4.5. Security

4.5.1. The Processor will:

4.5.1.1. Maintain appropriate organizational and technical security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, encryption of Personal Data while in transit and at rest) to protect against a Security Breach;

4.5.1.2. Be responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all of the Processor's personnel with respect to Personal Data and liable for any failure by such Processor personnel to meet the terms of this DPA;

4.5.1.3. Take appropriate steps to confirm that all of the Processor's personnel are protecting the security, privacy and confidentiality of Personal Data consistent with the requirements of this DPA; and

4.5.1.4. Notify the Controller of any Personal Data Breach by the Processor, its Sub-processors, or any other third parties acting on the Processor's behalf promptly and without undue delay, but in no event later than forty-eight (48) hours after becoming aware of a Personal Data Breach.

4.6. Additional Provisions for California Personal Information

4.6.1. When the Processor Processes California Personal Information in accordance with the instructions received from the Controller, the Parties acknowledge and agree that the Controller is a Business and the Processor is a Service Provider for the purposes of the CCPA. The parties agree that the Processor will Process California Personal Information as a Service Provider strictly for the purpose of providing the Processor's services (the "Business Purpose") as agreed with the Controller or as otherwise permitted by the CCPA.

5. Reviews, Audits and Certifications of Compliance

5.1. Each Party shall be able to demonstrate compliance with its respective obligations under this DPA and applicable Data Protection Laws. In particular,

each Party shall keep appropriate documentation of the Processing activities carried out under its responsibility pursuant to this DPA.

5.2. Each Party shall deal promptly and adequately with reasonable inquiries from the other Party about the Processing under this DPA.

5.3. Taking into account the nature of the Processing, each Party shall provide each other with reasonable assistance to the other Party in ensuring compliance with the following obligations, if applicable:

5.3.1. To carry out an assessment of the impact of the envisaged Processing on the protection of Personal Data (i.e., a 'privacy impact assessment,' and/or a 'data protection impact assessment') where a type of Processing is likely to result in a high risk to the rights and freedoms of Data Subjects; and

5.3.2. To consult the Data Protection Authority prior to engaging in a type of Processing where such impact assessment indicates that the Processing would likely result in a high risk in the absence of measures taken by each Party to mitigate the risk.

5.4. Each Party agrees to submit themselves to the jurisdiction of and cooperate with the Data Protection Authority in any procedures aimed at ensuring compliance with this DPA. In particular, each Party agrees to respond to inquiries, submit to audits and comply with the measures adopted or mandated by the Data Protection Authority, including remedial and compensatory measures. Where applicable and necessary, each Party shall provide such authority with written confirmation that the necessary actions have been taken.

6. Deletion Retention and Deletion

6.1. Each Party shall retain the Personal Data for no longer than is necessary to carry out the purpose(s) of Processing set forth in this DPA or as otherwise agreed with the Controller, and do so in accordance with applicable Data Protection Law. Each Party shall implement appropriate technical or organizational measures to ensure compliance with this obligation, including appropriate data retention policies and procedures, and mechanisms to securely delete, erase, destroy, dispose of, or anonymize the Personal Data.

6.2. Each Party may continue to retain the Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and/or industry, any documented backup policies and procedures, and/or as otherwise permitted by applicable Data Protection Law. During this retention period, the Party shall continue to treat the Personal Data in accordance with applicable Data Protection Law and shall not Process such data for purposes other than those set forth in this DPA.

7. Cross Border Transfers

7.1. Subject to each Party's data location commitments under the Joint Customer Agreement and the remainder of this Section 7 (Cross Border Transfers), Personal Data may be processed in any country in which a Party or its Subprocessors maintain facilities. Wherever Personal Data is transferred outside

its country of origin by one Party to the other Party, the Parties shall ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7.1.1. Partner Personal Data

7.1.1.1. For transfers of Partner Personal Data from Partner to Airship for Processing by Airship in a jurisdiction outside European Economic Area or the UK that does not provide an adequate level of protection for Personal Data (within the meaning of applicable EU Data Protection Laws), the Parties agree that:

7.1.1.1.1. *For Transfers from the EEA.* With respect to Partner Personal Data transferred from the European Economic Area, the SCCs incorporated herein by reference subject to the terms of Section 7.1.4 (*Additional Terms as to the SCCs*) shall apply and form part of this DPA. With respect to Partner Personal Data, the "data exporter" shall be Partner and the "data importer" shall be Airship (acting on behalf of itself and its Affiliates).

7.1.1.1.2. *Transfers from the UK.* With respect to Partner Personal Data subject to UK Data Protection Laws, the Parties conclude the UK Addendum, which is hereby incorporated into this DPA by reference, and Part 1 of the UK Addendum is completed as provided in Section 7.1.5 (*Additional Terms as to the UK Addendum*).

7.1.2. Airship Personal Data

7.1.2.1. For transfers of Airship Personal Data from Airship to Partner for Processing by Partner in a jurisdiction outside European Economic Area or the UK that does not provide an adequate level of protection for Personal Data (within the meaning of applicable EU Data Protection Laws), the Parties agree that:

7.1.2.1.1. *For Transfers from the EEA.* With respect to Airship Personal Data transferred from the European Economic Area, the SCCs incorporated herein by reference subject to the terms of Section 7.1.4 (*Additional Terms as to the SCCs*) shall apply and form part of this DPA. With respect to Airship Personal Data the "data exporter" shall be Airship (acting on behalf of itself and its Affiliates) and the "data importer" shall be Partner.

7.1.2.1.2. *Transfers from the UK.* With respect to Airship Personal Data subject to UK Data Protection Laws, the Parties conclude the UK Addendum, which is hereby incorporated into this DPA by reference, and Part 1 of the UK Addendum is completed as provided in Section 7.1.4 (*Additional Terms as to the UK Addendum*).

7.1.3. Joint Customer Personal Data

7.1.3.1. For transfers of Joint Customer Personal Data from one Party for Processing by the other Party in a jurisdiction outside European Economic Area or the UK that does not provide an adequate level of protection for Personal Data (within the meaning of applicable EU Data Protection Laws), the Parties agree that:

7.1.3.1.1. *For Transfers from the EEA.* With respect to Joint Customer Personal Data transferred from the European Economic Area, the SCCs incorporated herein by reference subject to the terms of Section 7.1.4 (*Additional Terms as to the SCCs*) shall apply and form part of this DPA. Depending on the circumstances, Airship may be the data exporter and Partner may be the data importer or Airship may be the data importer and Partner may be the data exporter as agreed under the Joint Customer Agreement;

7.1.3.1.2. *Transfers from the UK.* With respect to Joint Customer Personal Data subject to UK Data Protection Laws, the Parties conclude the UK Addendum, which is hereby incorporated into this DPA by reference, and Part 1 of the UK Addendum is completed as provided in Section 7.1.4 (*Additional Terms as to the UK Addendum*).

7.1.4. *Additional Terms as to the SCCs.* The SCCs are hereby completed as follows: (i) the Module One terms shall apply where both Parties are Controllers; (ii) the Module Two terms shall apply where the Party receiving Personal Data under the SCCs is acting as a Processor on behalf of the other party as a Controller; (iii) Module Three shall apply where both Parties are Processors and the Joint Customer is a Controller, and any election of specific terms and optional clauses described herein as to Module 2 and any Annexes included within the SCCs herein that may be applicable to Module 3 shall also apply to Module 3 to the extent applicable; (iv) in Clause 7, the optional docking clause shall apply; (v) in Clause 9, Option 2 of Module Two shall apply and the Processor shall obtain authorization for Subprocessors in accordance with the terms of this DPA or a Joint Customer Agreement, as applicable; (vi) in Clause 11, the optional language shall be deleted; (vii) in Clause 17 and Clause 18(b), the SCCs shall be governed by the laws of and disputes shall be resolved before the courts of the Republic of Ireland or the EEA member state in which the data exporter legal entity that has entered into the DPA is established; (viii) in Annex I of the SCCs, the details of the parties is set out in Annex I Subpart A to this DPA; and (ix) the remaining information in Annex I and Annex II of the SCCs shall be deemed completed with the information set out in Annex I Subpart B and of this DPA. In the event of a conflict between any provision of the SCCs and any provision of this DPA, the SCCs will control to the extent of conflicts.

7.1.5. *Additional Terms as to the UK Addendum.* In relation to Personal Data that is subject to the UK GDPR, the SCCs shall apply in accordance with Section 7.1.4 above and the following additional modifications: (i) the SCCs shall be amended as specified by the UK Addendum, which shall be incorporated by reference; (ii) Tables 1 to 3 in Part 1 of the UK Addendum shall be populated with relevant information set out in Schedule A of this DPA; (iii) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither"; and (iv) any conflict between the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

7.2. **Data Privacy Framework**. To the extent applicable, Airship complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Airship has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of Personal Data received from the EEA in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Airship has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. Where a Party is (a) located in the United States of America and is self-certified under the EU-U.S. DPF, the Swiss-U.S. DPF or the UK Extension to the EU-U.S. DPF as applicable, or (b) located in the EEA, Switzerland or the United Kingdom, as applicable, and transfers Personal Data to the other Party, the receiving Party agrees (i) to provide at least the same level of protection to any Personal Data as required by the applicable DPF Principles; (ii) to notify the transferring Party in writing, without undue delay, if its self-certification to the applicable DPF is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative Transfer Mechanism will apply in accordance with the order of precedence in Section 7.3 of this DPA); and (iii) upon written notice, to work with the transferring Party to take reasonable and appropriate steps to stop and remediate any unauthorized processing of Personal Data.

7.3. **Order of Precedence**. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism, as applicable, and in accordance with the following order of precedence: (a) the SCCs as set forth in this DPA; (b) the UK Addendum as set forth in this DPA; (c) the Data Privacy Framework as set forth in this DPA; and, if neither (a), (b), nor (c) is applicable, then (d) other applicable data Transfer Mechanisms permitted under applicable Data Protection Law.

8. CCPA/CPRA Terms.

8.1. *Service Provider Terms*. Where one Party acts as a "business" subject to the CCPA and the other Party acts as a "service provider" Processing Personal Data on behalf of the business, the following terms shall apply in addition to the other

pertinent terms of the Agreement and this DPA. The parties acknowledge and agree that with regard to any personal information the Processor may Process in accordance with the instructions received from the Controller, the Controller is a Business and the Processor is a Service Provider for the purposes of the CCPA. The parties acknowledge and agree that the Processor is a Service Provider for the purposes of the CCPA and is receiving personal information from the Controller pursuant to the Agreement for a Business Purpose. The Processor does not and will not: (i) Process Personal Data for its own purposes or those of any third party, including Processing Personal Data for its or a third party's own commercial purposes; (ii) retain, use, or disclose Personal Data for any purpose other than for the Business Purpose, including retaining, using, disclosing Personal Data for a commercial purpose other than for the Business Purpose specified in the Agreement or as otherwise permitted by applicable Data Protection Laws; (iii) sell or share any such Personal Data; or (iv) combine Personal Data with Personal Data that the Processor receives from or on behalf of another person, or collects from its own interactions with a Data Subject except only to the extent permitted under CCPA. The Processor will not retain, use or disclose any personal information provided by the Controller pursuant to the Agreement except as necessary for the specific purpose of performing the services for the Controller pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms "business," "personal information," "service provider," "sale," "share" and "sell" are as defined in the CCPA. The Processor certifies that it understands the restrictions of this paragraph.

8.2. *Business-to-Business Terms*. Where both Parties are acting as "businesses" subject to the CCPA and each Party is a Controller of Personal Data in a controller-to-controller scenario, the following terms shall apply:

8.2.1. Each Party represents and warrants that it is a "business" as defined under the CCPA and that it Processes Personal Data in compliance with the CCPA and other applicable Data Protection Laws.

8.2.2. Each Party agrees that any disclosure of Personal Data to the other Party pursuant to this DPA is made for a business purpose as defined under the CCPA and not for purposes of a "sale" or "share" of Personal Data as those terms are defined in the CCPA.

8.2.3. Each Party agrees that it will not "sell" or "share" (as those terms are defined in the CCPA) any Personal Data received from the other Party under this DPA except to the extent otherwise permitted under CCPA, or otherwise without the express written consent of the disclosing Party.

8.2.4. Each Party agrees to comply with all applicable requirements of the CCPA with respect to Personal Data it Processes under this DPA, including but not limited to providing appropriate notices to consumers, honoring consumer rights requests, maintaining reasonable security procedures and practices, and maintaining records of Processing activities as required by the CCPA.

8.2.5. Each Party agrees to reasonably cooperate with the other Party to enable compliance with consumer rights requests under the CCPA, including requests for access, deletion, correction, and opt-out of sale/sharing, where such requests relate to Personal Data Processed under this DPA.

8.2.6. Each Party shall notify the other Party promptly if it receives a consumer request under the CCCA that relates to Personal Data received from the other Party, and the Parties shall cooperate in good faith to respond to such requests in accordance with applicable law.

8.2.7. The Parties acknowledge that to the extent either Party acts as a "third party" (as defined in the CCPA) with respect to Personal Data received from the other Party, such Party shall not sell or share such Personal Data and shall comply with all restrictions applicable to third parties under the CCPA.

9. Term. This DPA shall remain in effect as long as either Party carries out Personal Data Processing operations on the Personal Data uploaded or otherwise provided by the other Party pursuant to and in accordance with the Partner Agreement or Joint Customer Agreement as applicable.

10. Indemnity. Subject to the limitation of liability terms of the applicable Partner Agreement, each Party shall defend, indemnify, and hold harmless the other and its subsidiaries, affiliates, and its respective officers, directors, employees, and agents from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against the other arising out of or resulting from the breaching party's failure to comply with any of its obligations under this DPA or the applicable Data Protection Laws. Each Party's liability shall be subject to the limitation of liability in the applicable Partner Agreement.

11. Relationship with the Agreement

11.1. Status of Agreement. The parties agree that this DPA will replace any existing data protection addendum or similar agreement the parties may have previously entered into in connection with the Services. Except for the changes made by this DPA, the Partner Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Partner Agreement, this DPA will prevail to the extent of that conflict.

11.2. Governing Law. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Partner Agreement, unless required otherwise by applicable Data Protection Laws as set forth in the Standard Contractual Clauses.

AIRSHIP GROUP, INC.	**PARTNER:**
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

ANNEX I

LIST OF PARTIES

Entity Name: Airship Group, Inc.

Address: 548 Market St., Suite 698370, San Francisco, California 94104-5401

Contact person's name, position and contact details: Neil Gariepy, VP Security and Infrastructure, privacy@airship.com

Activities relevant to the data transferred under these Clauses: The services defined in the Partner Agreement.

Signature and date: _____

Role (controller/processor): Controller or Processor depending on the Personal Data being provided as determined under the DPA above.

Partner Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: The services defined in the Partner Agreement.

Signature and date: _____

Role (controller/processor): Controller or Processor depending on the Personal Data being provided as determined under the DPA above.

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concerns the following categories of data subjects, depending on the Partner Agreement between the Airship and Partner, including the following:

Each Party's potential and actual customers; employees; and sales and marketing leads.

To the extent applicable to the Partner Agreement, Joint Customer's employee or end user or actual customer Personal Data.

Categories of personal data transferred

The data transferred is the personal data collected by each Party in connection with the services described in the Partner Agreement or to the extent applicable, the Joint Customer Agreement. Such personal data may include:

Describe any Sensitive data transferred (if applicable) and the 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.

Not applicable.

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis).

Personal data may be transferred from time to time in accordance with the Partner Agreement.

Nature of the processing

Each Party will process (including, collecting, recording, organizing, structuring, storing, altering, retrieving, using, disclosing, combining, erasing and destroying) personal data for the purpose of providing the services described in the Partner Agreement, or to the extent applicable Joint Customer Agreement.

Purpose(s) of the data transfer and further processing

The transfer is made for the following purposes: to facilitate the provision of the services described in the Partner Agreement, including as applicable to Joint Customers.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period for which the personal data will be retained will be determined by each Party in accordance with its respective data privacy and data retention policies.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As above.

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The EEA member state in which the data exporter legal entity that has entered into the DPA is established.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex II sets forth the technical and organisational measures that must be implemented and maintained by both Parties under this DPA, taking into account the nature, scope, context and purposes of Processing, the risks of varying likelihood and severity for rights and freedoms of natural persons, and the state of the art and costs of implementation. The specific measures applicable to each Party depend on their role as Controller, Processor, or Joint Processor in the various data sharing scenarios contemplated by this DPA.

SECTION I: GENERAL SECURITY STANDARDS

The following minimum technical and organisational security standards must be implemented and maintained by both Parties when Processing Personal Data under this DPA. These measures are designed to ensure a level of security appropriate to the risks presented by the Processing, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

A. Information Security Program and Attestations

Both Parties shall maintain a comprehensive information security program that includes regular security assessments, risk management processes, and governance structures appropriate to the scope and sensitivity of Personal Data processed. Where commercially reasonable and proportionate to the Processing activities, Parties should obtain relevant third-party security certifications or attestations such as SOC 2 Type II, ISO 27001, or equivalent standards.

B. Access Controls

Physical and logical access to Personal Data shall be restricted through appropriate access control measures, including:

a. Physical access controls to facilities containing Personal Data through security measures such as keycard systems, biometric authentication, security personnel, and visitor management procedures;

b. Logical access controls through role-based access management, multi-factor authentication for privileged accounts, regular access reviews, and prompt termination of access upon personnel changes.

C. Network Security

Network infrastructure Processing or transmitting Personal Data shall be protected through:

a. Encryption of Personal Data in transit using industry-standard protocols (TLS 1.2 or higher);
b. Network security monitoring and intrusion detection capabilities;
c. Protection against distributed denial of service (DDoS) attacks;
d. Network segmentation and firewall controls where appropriate;
e. Regular security monitoring and logging of network activities.

D. Application Security

Applications that Process Personal Data shall be developed and maintained according to secure development practices, including:

a. Implementation of secure coding standards and practices;
b. Regular security testing, code reviews, and vulnerability assessments;
c. Input validation and data sanitization procedures;
d. Protection against common application security vulnerabilities as identified in industry frameworks such as OWASP;
e. Secure configuration and patch management procedures.

E. ***Operational Security***

Operational security measures shall include:

a. System redundancy and failover capabilities appropriate to business requirements;
b. Regular vulnerability scanning and patch management processes;
c. Documented business continuity and disaster recovery plans that are tested periodically;
d. Change management procedures for systems Processing Personal Data;
e. Regular backup procedures and restoration testing.

F. ***Personal Data Protection***

Technical measures for protecting Personal Data shall include:

a. Encryption of Personal Data at rest using industry-standard encryption algorithms and key management practices;

b. Data minimization practices to ensure only necessary Personal Data is collected and retained;

c. Automated data retention and deletion procedures in accordance with applicable policies and legal requirements;

d. Technical capabilities to facilitate data portability and export as required by applicable Data Protection Laws;

e. Data integrity controls to prevent unauthorized alteration of Personal Data.

G. Data Breach Management

Each Party shall maintain documented procedures for detecting, investigating, and responding to Security Breaches, including:

a. Security incident detection and monitoring capabilities;

b. Incident response procedures with defined roles and responsibilities;

c. Notification procedures to ensure compliance with forty-eight (48) hour notification requirements under this DPA;

d. Documentation and reporting procedures for Security Breaches;

e. Remediation and lessons learned processes to prevent recurrence.

H. Personnel Security

All personnel with access to Personal Data shall be subject to appropriate security measures, including:

a. Background checks commensurate with the sensitivity of Personal Data accessed;

b. Confidentiality agreements covering data protection obligations;

c. Regular privacy and security awareness training;

d. Clear policies and procedures regarding acceptable use and data protection requirements;

e. Disciplinary procedures for violations of data protection policies.

I. Privacy by Design

Privacy and data protection considerations shall be integrated into system design and business processes, including:

a. Privacy impact assessments for Processing activities that may result in high risks to data subjects;

b. Implementation of privacy-enhancing technologies where appropriate and feasible;

c. Regular review of Processing activities for compliance with data minimization and purpose limitation principles;

d. Documentation of Processing activities as required by applicable Data Protection Laws

J. Sub-processor Security

When engaging Sub-processors for Personal Data Processing activities:

a. Appropriate due diligence and security assessments shall be conducted prior to engagement.

b. Written agreements shall require Sub-processors to implement equivalent security measures;

c. Ongoing monitoring and periodic review of Sub-processor security practices shall be maintained;

d. Clear procedures for Sub-processor notification and objection rights shall be established.

SECTION II: AIRSHIP SECURITY MEASURES

Airship's specific technical and organisational security measures that meet or exceed the standards set forth in Section I of this Annex are described in detail at https://www.airship.com/legal/security-measures/ and are hereby incorporated by reference into this DPA.

Airship maintains SOC 2 Type II certification covering security, availability, and confidentiality controls. These measures are regularly reviewed and updated to maintain effectiveness against evolving security threats and regulatory requirements.

SECTION III: PARTNER SECURITY MEASURES

Partner shall complete this section at the time of execution of this DPA or promptly thereafter to describe Partner's technical and organisational security measures that meet or exceed the standards set forth in Section I of this Annex.

[Partner to add in their Security Measures Annex here. The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page

of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.]

SECTION IV: UPDATES AND MODIFICATIONS

The security measures described in this Annex may be updated from time to time by either Party, provided that such updates do not result in a material degradation of the overall level of security and protection afforded to Personal Data. Any material changes to security measures that may affect the protection of Personal Data processed under this DPA shall be communicated to the other Party with reasonable advance notice. Each Party may, upon reasonable request and with appropriate confidentiality protections, provide the other Party with information necessary to demonstrate ongoing compliance with the security standards set forth in this Annex, including summaries of third-party certifications, completed security questionnaires, or other evidence of security controls implementation.

ANNEX III

LIST OF SUB-PROCESSORS

Airship's Subprocessors:

The specific subprocessors and the extent of data transfer is based on each customer's configuration and use of the Airship Services and is available at: https://www.airship.com/legal/subprocessors/

Data Controller may subscribe to receive updates to any subprocessor information by visiting https://www.airship.com/legal/subprocessors/ .

Partner's Sub-processors:
[Partner to fill in with their list of Subprocessors.]