Airship Group, Inc.

Checklist for Executing Data Processing Addendum ("DPA")

Airship's DPA consists of the following: (i) the main DPA Agreement; and (ii) the Standard Contractual Clauses (the "SCCs") and the UK Addendum as incorporated by reference in this DPA, which shall apply to the extent personal data subject to the SCCs or the UK Addendum is in scope of the Processing subject to this DPA.

This checklist helps guide you in the signature process of the DPA to demonstrate the parties are legally compliant and ensure a fully-executed DPA. Please note that the SCCs and the UK Addendum are standard legal documents provided by the EU and UK legal authorities, and not subject to revisions.

Relevant section in the DPA:	**Please sign/complete the following sections in the DPA:**
Section 9.2 (c)(x)	Fill in your selection of Supervisory Authority.
Following Clauses 1-12 of the DPA	Please sign the signature block, and complete the Customer's corporate entity name, along with the name and title of the Customer's signatory.
Annex I, Clause 9	Fill in with the name and contact email for your data protection team or DPO.

To sign on behalf of Airship Group, Inc. please send this DPA to:

Neil Gariepy
VP, Infrastructure & Security
neil.gariepy@airship.com copying in airshiplegal@airship.com

AIRSHIP DATA PROCESSING ADDENDUM

(*Version Date: January 13, 2026*)

This Data Processing Addendum ("DPA") forms part of the Main Subscription Agreement or the online Terms of Subscription Service (the "Agreement") between the customer that has executed this DPA and is an Airship customer on the date this DPA is fully executed ("Customer") and Airship. This DPA reflects the parties' agreement with regards to the processing of Customer Data in connection with Customer's use of the Service in accordance with the requirements of Data Protection Laws. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Airship processes Customer Data for which such Authorized Affiliates qualify as Data Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

In the course of providing the Service to Customer pursuant to the Agreement, Airship may process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions, each acting reasonably and in good faith. This DPA applies where and only to the extent that Airship processes Customer Data that is subject to Data Protection Laws on behalf of Customer as Data Processor in the course of providing Service pursuant to the Agreement.

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Airship**" means Airship Group, Inc. ("Airship"), a company incorporated in Delaware; Urban Airship UK Limited, a company registered in England and Wales; Airship France SAS, a company registered in France; Airship Business France SAS, a company registered in France;

Urban Airship Germany GmbH, a company registered in Germany; Urban Airship India Private, Ltd., a company registered in India; Apptimize LLC ("Apptimize"), and any other Affiliate of Airship.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws, and (b) is permitted to use the Service pursuant to the Agreement between Customer and Airship, but has not signed its own Order Form with Airship and is not a "Customer" as defined under the Agreement.

"**Customer Data**" means any Personal Data that Airship processes as a Data Processor on behalf of Customer or an Authorized Affiliate.

"**Data Controller**" means the entity which determines the purposes and means of the processing of Personal Data. Customer or its Authorized Affiliate is the Data Controller with respect to Customer Data.

"**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller, and includes similar terms used in Data Protection Laws, including "service provider" under the CCPA. Airship, including its Affiliates, is the Data Processor with respect to Customer Data under EU Data Protection Laws or as applicable under other Data Protection laws, and "service provider" under the CCPA.

"**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.

"**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

"**EEA**" means, for purposes of this DPA, the European Economic Area, Switzerland, and the United Kingdom.

"**EU Data Protection Laws**" means (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).

“**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").

“**ICO**” means the United Kingdom’s Information Commissioner’s Office.

“**Personal Data**” has the same meaning as the term “personal data” or “personal information” under the applicable Data Protection Laws, provided, that with respect to this DPA, the reference is to Personal Data processed in relation to Customer’s access to and use of the Service.

“**Process**” or “**Processing**” 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.

“**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 Customer Data.

“**Security Measures**” means the Security Measures applicable to the specific Service purchased by Customer described at https://www.airship.com/legal/security-measures/ .

“**Service**” means, the Airship Services and the Apptimize Services described in the Documentation and procured by Customer, and any other services provided by Airship as described under the Agreement.

“**Standard Contractual Clauses**” or “**SCCs**” means the Standard Contractual Clauses implemented by European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council and incorporated herein by reference as further completed in Section 9.2 (Data Transfers from the EEA under the SCCs) of this DPA, and the UK Addendum where applicable.

"**Sub-processor**" means any Data Processor or Service Provider engaged by Airship to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA.

"**UK Addendum**" means the International Data Transfer Addendum issued by the ICO to the EU Commission's Standard Contractual Clauses VERSION B1.0, in force 21 March 2022 and incorporated herein by reference as further completed in Section 9.3 (Data Transfers from the UK under the SCCs) of this DPA .

"**Transfer Mechanism**" means an onward transfer mechanism, to the extent Customer's use of the Services requires the lawful transfer of Personal Data from a jurisdiction (i.e., the EEA, the United Kingdom, Switzerland, or any other jurisdiction listed in this DPA) to an Airship entity located outside of that jurisdiction. The terms set forth in Section 9 (International Transfers) of this DPA will apply to such Transfer Mechanism.

The terms, "**Member State**", and "**Supervisory Authority**" shall have the same meaning as in the applicable Data Protection Laws, and their cognate terms shall be construed accordingly. The terms "**Sell**", "**Share**" and "**Service Provider**" shall have the meanings assigned under CCPA, and their cognate terms shall be construed accordingly. All other capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller of Customer Data, and Airship shall act as a Data Processor or Service Provider and shall Process Customer Data only on the instructions of Customer, unless as otherwise specifically agreed below.

2.2 Customer's Processing of Customer Data. Customer shall (i) comply with the Data Protection Laws and its obligations as a Data Controller under the Data Protection Laws in respect of its use of the Service and any Processing instructions issued to Airship, and (ii) maintain legally adequate privacy policy and notices for each mobile application, web domains, devices, software applications and/or communication channels owned or controlled by the Data Controller or its Affiliate that connects to the Service, (iii) provide notice, respond to individual rights requests, and obtain all legally required rights, releases and consents (including as required under Health Privacy Laws for any applicable Personal Data) to allow Customer Data to be collected, processed, stored, used, transmitted and disclosed in the manner contemplated by the Agreement and this DPA, (iv) implement appropriate technical and organizational measures to protect sensitive Personal Data, and (v) unless otherwise specifically agreed to herein, not use the Service to Process any government issued ID numbers such as passport numbers, individual medical or health information, 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”). Customer shall have sole responsibility for the (1) accuracy and quality of Customer Data, (2) for obtaining the appropriate permissions for legally processing and using the Customer Data, and (3) for the means by which Customer acquires and uses Customer Data as contemplated under the Agreement and this DPA (including, without limitation, any Customer Data sent to, provided by or accessed by a Third Party Application that Customer links to the Service). Where Customer’s processing is subject to Health Privacy Laws, Customer is responsible for determining whether any Personal Data it processes through the Airship Service constitutes health data under applicable Health Privacy Laws and for ensuring Customer’s own compliance with such Health Privacy Laws. Customer is also responsible for informing Data Subjects, notably End Users, of the use by Airship, acting as a Data Controller of Aggregate Usage Data for the purposes of the processing detailed under Section 2.5 below.

2.3 Airship’s Processing of Customer Data. Without prejudice to Section 2.5 below, Airship shall only process Customer Data on behalf of and in accordance with Customer’s instructions, or as otherwise allowed by Data Protection Laws, for the period set out in the Agreement. Instructions by Customer to Airship to process Customer Data include: (i) processing in accordance with the Agreement and applicable Order Form(s); (ii) processing initiated by Account Users in their use of the Service; (iii) processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; and (iv) processing in accordance with all configuration of the Service by or for Customer, (together, the “Business Purpose”). Airship shall, as soon as reasonably practicable upon becoming aware of receiving such instruction, inform Customer if, in Airship’s opinion, any instructions provided by Customer under this clause infringe applicable Data Protection Laws. Furthermore, Customer agrees that Airship may use the Aggregated Service Data to provide the Customer with the functionalities in the Service. For clarity, this section and the terms of the Aggregate Data section of the Agreement do not give Airship the right to use the Aggregated Service Data to identify an individual, an End User, or Customer as the source of any Aggregated Service Data, and Airship shall not sell or disclose the raw data or personal data included in the Aggregated Service Data to any third party. Airship shall not combine Aggregated Service Data from Customer’s account with other Airship customers’ End User data.

2.4 Details of Data Processing. The details of data processing, including the subject matter, duration of processing, purpose of processing, nature of processing, and categories of Data Subjects are set forth in Annex I to this DPA, (“Annex I”). For clarity, Annex I describes all Processing of Personal Data under this DPA under any applicable Data Protection Laws and is not limited to the EU Data Protection Laws. The types of Customer Data processed are described in detail in Annex I, and may include:

A. Customer and Account Users: Account User’s login credentials to the Service;
B. End Users: Customer determines the extent of Personal Data processed via the Services based on Customer's configuration and use of the Services. The specific

categories of Personal Data processed will vary according to the Services package subscribed to by Customer and the specific functionalities utilized. The specific categories of Personal Data processed will depend on Customer's implementation choices, the features and functionalities activated within Customer's Services, and Customer's data collection practices set up via the Customer's Digital Assets. Personal Data processed may include, but is not limited to:

1. Contact and identification information: Push tokens, email addresses, mobile phone numbers and Mobile Station International Subscriber Directory Number ("MSISDNs"), names, online identifiers, and unique user IDs;
2. Technical and device information: IP addresses, device information, browser data, location data (when Customer has enabled location-based features via a Third Party Application), and usage analytics;
3. Cross-channel engagement data: Information collected and processed across multiple communication channels including push notifications, in-app messaging, mobile app experiences, email, SMS/MMS, and mobile wallet;
4. Interactive data: Information collected through Customer's use of Scenes or Surveys functionalities, including user responses, preferences, and behavioral data; and
5. Any additional Personal Data that Customer chooses to collect and process through the Service, including through Tags and Events.

.

C. Special classes of data. Unless explicitly agreed and stated in the Annex I, Customer is contractually prohibited from processing via the Services any "special categories of data" as defined in Data Protection Laws as well as any Prohibited Data.

2.5 Subsequent processing of Aggregated Usage Data by Airship. Customer agrees that Airship may use the Aggregated Usage Data to analyze, improve, develop, and support and operate the Service performance, and to prepare and distribute to Airship's customers and publish on Airship's blogs and websites general benchmarking and industry reports derived from Aggregated Usage Data. For clarity, this section and the terms of the Aggregate Data section of the Agreement do not give Airship the right to use the Aggregated Usage Data to identify an individual, an End User, or Customer as the source of any Aggregated Usage Data, and Airship shall not sell or disclose the raw data or personal data included in the Aggregated Usage Data to any third party.

3. RIGHTS OF DATA SUBJECTS AND COOPERATION

3.1 Data Subject Requests. Airship will comply fully with the requirements of applicable Data Protection Laws, and where applicable as required under EU Data Protection Laws, Clause 10 and Clause 11 of the Standard Contractual Clauses. The Service provides Customer with a number of controls that Customer may use to retrieve, correct, delete, or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the Data Protection

Laws including, for example, its obligations relating to responding to Requests from Data Subjects or applicable data protection authorities as provided here. To the extent Customer is unable to independently access the relevant Customer Data within the Service, Airship will provide reasonable cooperation to assist Customer, at Customer's cost to the extent legally permissible, to respond to any requests from Data Subjects or applicable data protection authorities relating to the processing of Customer Data under the Agreement and this DPA. In the event any such request is made directly to Airship, Airship will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Airship is required to respond to such a request, Airship will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

3.2 Records of Processing. The Service provides Customer with the ability to access certain Customer Data to provide records of processing. To the extent Customer is unable to independently access the relevant records of processing of Customer Data within the Service, Airship will provide reasonable cooperation to assist Customer in a timely manner as is required by Customer to demonstrate Airship's compliance with its obligations under the Data Protection Laws and under this DPA.

3.3 Government or Other Public Authority Requests. With regard to government body or agency legally enforceable demands for Customer Data, Airship will comply fully with Airship's Policy on Response to Public Authority Requests for Personal Data available here and the applicable requirements of Data Protection laws, including where applicable under EU Data Protection Laws with Clause 14 and Clause 15 of the Standard Contractual Clauses. If any government agency or body sends Airship a legally enforceable demand for Customer Data (for example, a subpoena or a valid court order), Airship will attempt to redirect the government agency or body to request that data directly from Customer to the extent permitted under Applicable Laws.

3.4 Data Protection Impact Assessments. To the extent Airship is required under Data Protection Laws, Airship will provide reasonably requested information regarding the Service to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

4. AIRSHIP PERSONNEL

Airship shall ensure that its personnel engaged in the processing of Customer Data are informed of the confidential nature of the Customer Data and have executed written confidentiality agreements. Airship shall ensure that its employees' confidentiality obligations survive the termination of their engagement. Airship shall ensure that Airship's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Airship's Affiliates may be retained as Sub-processors; and (b) Airship may engage third-party Sub-processors in connection with the provision of the Service. Airship has entered or shall enter as to new Subprocessors added in accordance with the terms of this Section 5 into a written agreement with each Sub-processor containing data protection obligations not less protective than those described in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Service provided by such Sub-processor. Airship makes available to Customer the current list of Sub-processors for the Service in Annex III to this DPA, ("Annex III") and by posting that list online at: https://www.airship.com/legal/subprocessors. If Customer wishes to receive automated notifications of pending changes and updates to Sub-processors in accordance with this section, then Customer must subscribe to receive automated notifications by signing up via the webform made available at : https://www.airship.com/legal/subprocessors.

5.2 Objection Right for New Sub-processors. If Customer has a reasonable basis to object to Airship's use of a new Sub-processor, Customer shall notify Airship promptly in writing within fourteen (14) days after receipt of Airship's notice regarding such new Sub-processor. In the event Customer objects to a new Sub-processor(s) on a reasonable basis, Airship will use reasonable efforts to work in good faith with Customer to find an acceptable, reasonable, alternate solution. If the parties are not able to agree to an alternate solution within a reasonable time (no more than 30 days), Customer may terminate the applicable Order Form(s) in respect only to the specific Service which cannot be provided by Airship without the use of the objected-to new Sub-processor, by providing written notice to Airship.

6. SECURITY

6.1 Controls for the Protection of Customer Data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Airship shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, the measures described in the Security Measures available at https://www.airship.com/legal/security-measures/ (the "Security Measures"), which are as set forth also in Annex II to this DPA ("Annex II"). Customer is responsible for reviewing the information made available by Airship relating to data security and making an independent determination as to whether the Service meets Customer's requirements. Customer acknowledges that the Security Measures are subject to technical progress and development and that Airship may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by the Customer.

6.2 Third-Party Certifications. Airship has obtained the third-party compliance audits set forth in the Security Measures. Upon Customer's written request at reasonable intervals, Airship shall provide an executive summary of Airship's then most recent third-party audits or certifications,

as applicable, that Airship generally makes available to its customers at the time of such request.

6.3 Customer Responsibilities. Notwithstanding the above, Customer agrees that except to the extent expressly provided in this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service in accordance with Applicable Laws and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Service.

6.4 Audits. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Airship shall promptly make available to Customer information regarding Airship's compliance with the obligations set forth in this DPA which may include one or more of the following as Customer may request: (i) responses to a reasonable information security-related questionnaire; (ii) copies of relevant executive summaries of the third-party certifications and compliance audits described in Section 6.2 of this DPA; (iii) a summary of Airship's operational practices related to data protection and security; and (iv) making Airship personnel reasonably available for security-related discussions with Customer. If Customer determines that information provided in accordance with the preceding methods is insufficient, then Customer may contact Airship in accordance with the "Notices" Section of the Agreement to schedule an on-site audit at Airship's designated facility of the procedures relevant to the protection of Customer Data. Customer shall reimburse Airship for any time expended for any such on-site audit at the Airship's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Airship shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify Airship with information regarding any non-compliance discovered during the course of an audit. For clarity, the audits referenced hereunder do not include any audits of Airship's Sub-processors.

7. DATA BREACH MANAGEMENT AND NOTIFICATION

Airship maintains data breach management policies and procedures specified in the Security Measures and shall, to the extent permitted by law, notify Customer without undue delay (no more than 48 hours of becoming aware) of any actual breach of security of the Service leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on the Service of which Airship becomes aware (a "Data Breach") and provide details of the Data Breach to the Customer.

8. DELETION OF CUSTOMER DATA

Airship shall delete Customer Data in accordance with the procedures and timeframes specified in the Agreement and the Data Retention Schedule available online at: https://docs.airship.com/reference/general/#data-retention-schedule. In addition, and as needed, Customer may request that Airship delete Customer Data at any point during the Term

of the Agreement. The parties agree that the certification of deletion of Customer Data shall be provided by Airship to Customer only upon Customer's written request. Within ninety (90) days of termination or expiration of the Agreement, Airship will delete all Customer Data (including copies) in its possession or control, save that this requirement will not apply to the extent Airship is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Airship will securely isolate and protect from any further processing, except to the extent required by applicable law.

9. INTERNATIONAL TRANSFERS

9.1 Processing Locations. To the extent necessary to provide Customer with the Services, Customer authorizes Airship and its Sub-processors to transfer Customer Data across international borders, including from the EEA, Switzerland or the United Kingdom to the United States. Airship stores Customer Data in the United States or in the European Union, based on the selection made by the Customer as specified on the applicable Order Form. If no location is stated on the Order Form, Airship stores Customer Data in the United States. For purposes of providing the Service, Customer Data may transfer from the originating location of Customer Data to the Service located in the United States or the European Union, as applicable. Additionally, for purposes of providing the Service including technical support, error fixes and operation purposes, Customer Data may be accessed from or relevant parts of Customer Data copied to locations where Airship's Affiliates are located.

9.2 Data Transfers from the EEA under the SCCs. Customer authorizes Airship and its Sub-processors to transfer Customer Data across international borders, including from the EEA or Switzerland to the United States, under a Transfer Mechanism recognized by the European Commission or the Swiss Federal Data Protection and Information Commissioner , as applicable. In the event that that any Customer Data originating in the EEA or Switzerland is transferred by Customer to Airship in a country that has not been found to provide an adequate level of protection under Data Protection Laws, the parties agree that the terms of the transfer shall be governed by the SCCs as incorporated here by reference. Each party's signature to the DPA shall be considered a signature to the SCCs to the extent that the SCCs are incorporated into this DPA by this reference. For purposes of this DPA, the SCCs are completed as follows and each party's signature to this DPA shall be considered a signature to the SCCs to the extent that the SCCs apply hereunder:

(a) Module Two (Controller to Processor) of the Standard Contractual Clauses will apply where Customer is a controller of Customer Data and Airship is processing Customer Data;

(b) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Data and Airship is processing Customer Data;

(c) For each Module, where applicable:

(i) in Clause 7 of the SCCs, the optional docking clause will apply;
(ii) the audits described in Clause 8.9 and Clause 13(b) of the SCCs shall be carried out in accordance with Section 6.4 of this DPA;
(iii) pursuant to Clause 9 of the SCCs , Airship may engage new Sub-processors in accordance with Section 5 of this DPA;
(iv) the certification of deletion referenced in Clause 8.5 and Clause 16(d) of the SCCs shall be provided only upon Customer's written request.
(v) in Clause 11 of the SCCs, the optional language will not apply;
(vi) In Clause 17 (Option 1), the SCCs will be governed by the law of the Netherlands;
(vii) in Clause 18(b) of the SCCs, disputes will be resolved before the courts of Netherlands
(viii) in Annex I, Part A of the SCCs:

Data Exporter: Customer
Contact Details: The email address(es) designated by Customer in Section 9 of Annex I;
Data Exporter Role: The Data Exporter's role is set forth in Section 2.1 (Role of the Parties) of this DPA;
Signature and Date: By entering into the DPA, Data Exporter is deemed to have signed these SCCs incorporated herein, including their Annexes, as of the effective date of the Agreement.

Data Importer: Airship Group, Inc.
Contact Details: Airship Privacy Team – privacy@airship.com
Data Importer Role: The Data Importer's role is set forth in Section 2.1 (Role of the Parties) of this DPA.
Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these SCCs, incorporated herein, including their Annexes, as of the effective date of the Agreement;

(ix) in Annex I, Part B of the SCCs:

The categories of data subjects are set forth in Section 1 of Annex I (Details of Processing) of this Addendum.

The Sensitive Data transferred is set forth in Section 3 of Annex I (Details of Processing) of this Addendum.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is set forth in Section 5 of Annex I (Details of Processing) of this Addendum.

The purpose of the processing is set forth in Section 6 of Annex I (Details of Processing) of this Addendum.

The period for which the personal data will be retained is set forth in Section 4 of Annex I (Details of Processing) of this Addendum.

For transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth Section 8 of Annex I (Details of Processing) of this Addendum.

(x) in Annex I, Part C of the SCCs: _____ will be the competent supervisory authority; and
(xi) Annex II (Technical and Organizational Security Measures) serves as Annex II of the SCCs.

9.3 Data Transfers from the UK under the SCCs. In case of any transfers of Personal Data under this DPA under the SCCs from the United Kingdom, to the extent such transfers are subject to UK Data Protection Laws , the Parties agree that the terms of the transfer shall be governed by the UK Addendum. For data transfers from the United Kingdom that are subject to the UK Addendum, the UK Addendum will be deemed entered into, and incorporated into this DPA by this reference, and completed as follows:

(a) The UK Addendum is subject to this DPA and the Agreement, forms an integral part of this DPA, and reflects the Parties' agreement with respect to the processing of UK Personal Data.
(b) The Parties hereby agree that Table 1, 2 and 3 of the UK Addendum will be deemed completed with the information about the version of the approved SCCs, applicable modules, and selected clauses, which the UK Addendum is appended to, and as set forth in Section 9.2 (Data Transfers from the EEA under the SCCs) of this DPA. Table 4 will be deemed completed by selecting "neither party".
(c) The parties agree that any reference to the SCCs shall refer to the SCCs together with the UK Addendum for the purposes of Personal Data subject to UK Data Protection Laws.
(d) For the purposes of the UK Addendum, the Customer shall be deemed to be the "data exporter" and Airship shall be deemed to be the "data importer".
(e) The parties agree that: (i) the audits described in Clause 8.9 and Clause 13(b) of the EU SCCs shall be carried out in accordance with Section 6.4 of this DPA; and (ii) pursuant to Clause 9 of the EU SCCs, Airship may engage new Sub-processors in accordance with Section 5 of this DPA; and (iii) the certification of deletion referenced in Clause 8.5 and Clause 16(d) of the SCCs shall be provided only upon Customer's written request. Each party's signature to the DPA shall be considered a signature to the SCCs to the extent that the SCCs apply hereunder.

(f) If there is any conflict between the UK Addendum and the DPA, the UK Addendum shall control and the conflict will be resolved in accordance with Section 10 and Section 11 of the UK Addendum

9.4 Data Privacy Framework. 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. To the extent that Customer 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, Airship further agrees (i) to provide at least the same level of protection to any Personal Data as required by the EU-U.S. DPF, the Swiss-U.S. DPF or the UK Extension to the EU-U.S. DPF Principles; (ii) to notify Customer in writing, without undue delay, if its self-certification to the EU-U.S. DPF, the Swiss-U.S. DPF or the UK Extension to the EU-U.S. DPF as applicable 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 9.5 (Order of Precedence) of this DPA; and (iii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of Personal Data.

9.5 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 Section 9.2 (Data Transfers from the EEA under the SCCs) of this DPA; (b) the UK Addendum as set forth in Section 9.3 (Data Transfers from the UK under the SCCs) of this DPA; (c) the Data Privacy Framework as set forth in Section 9.4 (Data Privacy Framework) of this DPA; and, if neither (a), (b), nor (c) is applicable, then (d) other applicable data Transfer Mechanisms permitted under applicable Data Protection Law.

9.6 Amendments to Address Changes in Data Protection Laws. Notwithstanding anything to the contrary, this Section 9 and the SCCs (including its appendices) may be amended by Airship to address changes in Data Protection Laws with fifteen (15) days' notice to Customer.

9.7 Legacy Standard Contractual Clauses. Customer agrees that, as of their effective date, the Standard Contractual Clauses entered into under this current Data Processing Agreement will supersede and terminate any Standard Contractual Clauses approved under Article 26(2) of Directive 95/46/EC and previously entered into by Customer with Airship, ("Former SCCs"). Where Airship is not a party to the Agreement, Airship will be a third party beneficiary of this Section 9.7 (Legacy Standard Contractual Clauses). This Section 9.7 will not affect either party's rights, or any data subject's rights, that may have accrued under the Former SCCs while they were in force.

10. CCPA TRANSFERS

Where Customer is a “business” subject to the CCPA, the following section shall apply in addition to the other pertinent terms of the Agreement and this DPA. The parties acknowledge and agree that Airship is a Service Provider for the purposes of the CCPA and is receiving personal information from Customer pursuant to the Agreement for a Business Purpose. Airship 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 Airship 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 and in accordance with the terms of Section 2 of this DPA (Processing of Personal Data). Airship will not retain, use or disclose any personal information provided by Customer pursuant to the Agreement except as necessary for the specific purpose of performing the services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. “Business Purpose” means instructions by Customer to Airship to Process Customer Data including: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Account Users in their use of the Service; (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; and (iv) Processing in accordance with all configuration of the Service by or for Customer.The terms “business,” “personal information,” “service provider,” “sale,” “share” and “sell” are as defined in the CCPA. Airship certifies that it understands the restrictions of this paragraph.

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 Service. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA will prevail to the extent of that conflict.

11.2 Claims. Any claims brought under or in connection with this DPA will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. Other than liability that may not be limited under applicable law, each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the ‘Limitation of Liability’ section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all Addenda together.

11.3 No Third Party Beneficiary. Other than the Data Subject rights set forth in Clause 3 of the Standard Contractual Clauses, no one other than a party to this DPA, its successors and permitted assignees will have any right to enforce any of its terms. Any claims against Airship or its Affiliates under this DPA will be brought solely against the entity that is a party to the Agreement. In connection with Clause 12(f) of the Standard Contractual Clauses, Customer further agrees that any regulatory penalties or other liability incurred by Airship in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws will count toward and reduce Airship's liability under the Agreement as if it were liability to the Customer under the Agreement.

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

12. LEGAL EFFECT

This DPA shall only become legally binding between Customer and Airship when executed as described in the introductory paragraphs to this DPA.

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

ANNEX I

DETAILS OF PROCESSING

1. Categories of data subjects whose personal data is processed:

Any individual accessing and/or using the Services through the Customer's Account as authorized by Customer ("Account Users"); and any end user of a Digital Asset, or other mobile application, web domains, devices, software applications and/or communication channels owned or controlled by Customer and to or with respect to whom Customer sends Notifications or Processes Personal Data via the Service (collectively, "End Users").

2. Categories of personal data processed:

Customer and Account Users: Account User's login credentials to the Service.

End Users: The specific categories of Personal Data Processed will depend on Customer's implementation choices, the features and functionalities activated within Customer's Services, and Customer's data collection practices set up via the Customer's Digital Assets. Personal Data Processed is:

1. Contact and identification information: Push tokens, email addresses, mobile phone numbers and Mobile Station International Subscriber Directory Number ("MSISDNs"), names, online identifiers, and unique user IDs;
2. Technical and device information: IP addresses, device information, browser data, location data (when Customer has enabled location-based features via a Third Party Application), and usage analytics;
3. Cross-channel engagement data: Information collected and processed across multiple communication channels including push notifications, in-app messaging, mobile app experiences, email, SMS/MMS/RCS, and mobile wallet;
4. Interactive data: Information collected through Customer's use of Scenes or Surveys functionalities, including user responses, preferences, and behavioral data;
5. Data related to RCS Notifications: If Customer elects to use the RCS Service, Airship will Process Personal Data necessary to deliver RCS Notifications, which include mobile phone numbers (MSISDNs), message content, sender identification, opt-in/opt-out status, and delivery metadata, as determined by Customer's configuration and use of the Service. Airship does not control or determine whether a Notification is delivered to an End User as an SMS Notification or as an RCS

Notification; this determination is made by the underlying telecommunications network or provider based on device and carrier capabilities in accordance with the Services the Customer has subscribed to with Airship. Accordingly, the categories of Personal Data processed for SMS Notifications and RCS Notifications may overlap, and all such processing is governed by this DPA; and

6. Any additional Personal Data that Customer chooses to collect and process through the Service, including through Tags and Events.

3. **Sensitive data processed:**

Customer is contractually prohibited from Processing via the Service any sensitive data as well as any individual financial data, credit or debit card numbers, individual health information, or government issued identification numbers.

4. **The duration of processing (eg. whether the data is processed on a one-off or continuous basis).**

Ongoing during the term of the Agreement.

5. **Nature of the processing:**

To carry out the obligations and perform the Services in accordance with the terms of the Agreement.

6. **Purpose(s) of the processing:**

To carry out the obligations and perform the Services in accordance with the terms of the Agreement.

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

For the duration of the Agreement and thereafter as set forth in Data Processor's data retention schedule which can be found at: https://docs.airship.com/reference/general/.

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

For the duration of the Agreement and as described in Data Processor's sub-processor descriptions which can be found at: https://www.airship.com/legal/subprocessors/.

9. **Identify the contact details of the data protection officer and/or privacy team:**

   Name:

   Email Address:

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

The Airship Security Measures in this Annex describe the technical and organisational measures Airship implemented to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

For purposes of the SCCs and the UK Addendum, the Standard Contractual Clauses implemented by European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 include the examples of possible technical and organizational measures below with the corresponding Airship Security Measures mapped alongside each example for reference:

- ***Measures of pseudonymisation and encryption of personal data:*** Airship Security Measures included in Sections 6(b), 6(c), 7(c), and 7(f).
- ***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:*** Airship Security Measures included in Sections 4(b), 5(a), 5(c), and 6(b).
- ***Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:*** Airship Security Measures included in Sections 6(a), 6(c), and 7(g).
- ***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:*** Airship Security Measures included in Sections 2, and 5(b).
- ***Measures for user identification and authorisation:*** Airship Security Measures included in Section 3(b).
- ***Measures for the protection of data during transmission:*** Airship Security Measures included in Section 4(a).
- ***Measures for the protection of data during storage:*** Airship Security Measures included in Sections 3(a), and 7(a).
- ***Measures for ensuring physical security of locations at which personal data are processed:*** Airship Security Measures included in Sections 3(a), 3(b), and 9.
- ***Measures for ensuring events logging:*** Airship Security Measures included in Section 3(b).
- ***Measures for ensuring system configuration, including default configuration:*** Airship Security Measures included in Section 5.
- ***Measures for internal IT and IT security governance and management:*** Airship Security Measures included in Section 2.
- ***Measures for certification/assurance of processes and products:*** Airship Security Measures included in Sections 2, and 5(b).
- ***Measures for ensuring data minimisation:*** Airship Security Measures included in Sections 7(b) and 10.
- ***Measures for ensuring data quality:*** Airship Security Measures included in Sections 2, 5, and 7.
- ***Measures for ensuring limited data retention:*** Airship Security Measures included in Section 7(c)
- ***Measures for ensuring accountability:*** Airship Security Measures included in Sections 7(e) and 11, and the Airship Policy on Response to Public Authority Requests for Personal Data.

- ***Measures for allowing data portability and ensuring erasure:*** Airship Security Measures included in Sections 7(c), and 7(d).

For transfers to Sub-processors, the specific technical and organisational measures applicable for each Sub-Processor are as described in Section 5 of the Airship Data Processing Agreement and as listed for each Sub-Processor at https://www.airship.com/legal/subprocessors.

AIRSHIP SECURITY MEASURES

Airship shall maintain appropriate technical and organizational measures for the Service to ensure a level of security appropriate to that risk, including, the measures described in this document (the "Security Measures"). Airship may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service.

1. Definitions

"Airship" means Airship Group, Inc. and its operating divisions, subsidiaries, affiliates and branches.

"Customer Data" means electronic data and content processed by Airship via the Service or provided to Airship by or for Customer via the Service.

"Data Breach" means a breach of security of the Service leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Customer Data in the Service.

"Service" means the Airship Service, the Apptimize Service ("Apptimize"), and any other services or functionalities related to either the Airship Service or Apptimize.

"SOC2 Report" means a confidential Service Organization Control (SOC) 2 Type II report (or a comparable report) on the Service examining logical security controls, physical security controls, and system availability, as produced by a Third-Party Auditor in relation to the Service.

"Third Party Auditor" means an Airship-appointed, qualified and independent third-party auditor.

Any other terms not defined herein shall have the meaning provided in the Agreement entered into with the Customer.

2. Information Security Program and Attestations

Airship maintains a robust information security program aligned with industry best practices (NIST, ISO 27001:2022) that includes the adoption and enforcement of internal policies and procedures. This program encompasses threat intelligence, vulnerability management, incident response, and continuous monitoring

and improvement, designed to (a) satisfy these Security Measures, (b) identify reasonably foreseeable security risks and unauthorized access to the Service, and (c) minimize security risks, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons. A Third-Party Auditor assesses the Airship Service (which includes mobile app, email, API, and SMS solutions, and Apptimize) annually for compliance with the SOC 2 Type II availability, confidentiality, and security trust principles. The Third-Party Auditor issues a SOC2 Report, which is available to the Customer upon request under signed NDA. The Airship SOC2 Report includes the cloud provider subprocessors used by Airship, but not the other subprocessors.

3. Access Controls

(a) Data Center Access Controls.

- Leading Cloud Data Centers. Airship uses Cloud Platform (Google Cloud) or for certain Airship customers, depending on location or the Airship services subscribed to, Amazon Web Services (AWS), to provide infrastructure services to host and operate the Service. By using Google Cloud's Trusted Infrastructure or AWS's Security, Identity, and Compliance Service, Airship is able to take advantage of their sophisticated security environments.
- Physical Access Control. The cloud data centers used to provide the Service are Tier 4 certified, ISO 27001, and SOC 2 Type II certified computing facilities. These cloud data center facilities maintain on-site security operations responsible for all physical data center security functions 24 hours a day, 7 days a week, with CCTV monitoring and access controls. The CCTV monitoring footage is kept for 90 days.

(b) Logical and Data Access Controls.

Infrastructure Security Personnel. Airship's dedicated infrastructure security team is responsible for the ongoing monitoring of Airship's security infrastructure, review of the Service, and security incident response.

Privilege Management. Airship personnel with access to the Airship customer account or technical management systems are required to authenticate themselves via logical access controls with multi-factor authentication in order to administer the Service. Any access to customer data by an Airship representative is logged and tracked in real time, with oversight from the security team. In addition, Airship has implemented these additional privilege management measures:

- Internal Data Access Processes and Policies. Airship's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process data in the Service.
- Access Management. Airship employs a centralized access management system to control personnel access to production servers for the Service to a limited number of authorized personnel.

Central network-based authentication systems are designed to provide Airship with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information for the Service. Airship requires the use of unique user IDs, strong passwords, two factor authentication and access lists for Airship personnel to access the Service. Airship personnel are granted access rights to the Service based on: (i) the authorized personnel's job responsibilities; (ii) job duty requirements necessary to perform authorized tasks based on least privilege; and (iii) a need-to-know basis. The granting or modification of access rights must be performed in accordance with Airship's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Log-ins to the Service are logged into the Security Information and Event Management system (SIEM).

- Access Controls. Security events for the Service, including login failures, use of privileged accounts, changes to access models or file permissions, modifications to installed software or operating systems, changes to user permissions or privileges are logged on the relevant systems. Logs are generated through monitoring and alerting systems, and are held from 30 days to 1 year, depending on the system. Airship implements Zero Trust principles, assuming that every access request, whether internal or external, could be a potential threat.

(c) Remote Access

Airship enforces secure remote access practices, including the use of multi-factor authentication (MFA) for all remote connections and virtual private networks (VPNs).

4. Network Security

(a) Data Transmission. Airship makes HTTPS encryption (also referred to as TLS connection) available for data in transit to or from the Service. Clear text HTTP connections to the Service are disabled by default. Airship employs network segmentation to isolate sensitive data and limit the impact of potential incidents.

(b) Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. The intrusion detection measures used by Airship involve:

- controlling the size and make-up of Airship's attack surface through preventative measures;
- employing intelligent detection controls at data entry points; and
- employing technologies that automatically remedy certain dangerous situations.

Network traffic is continuously monitored and analyzed using advanced tools to detect and respond to anomalies and potential threats. Airship also implements robust DDoS protection and mitigation strategies to ensure service availability.

5. Application Security

(a) Software Development. Airship follows a secure Software Development Lifecycle (SDLC) that includes threat modeling, secure coding practices, and rigorous security testing (SAST, DAST, IAST). This code is reviewed and approved based on peer review prior to staging the code. All development for the Service is based on the SDLC model in accordance with Airship's development policies.

(b) Standards Compliance. Airship adheres to an "out of the box" default security standard in alignment with OWASP Top 10 best practices, CIS controls, and SOC2 Type II principles.

(c) Data Integrity. Measures are in place to prevent corruption of stored Customer Data due to a malfunctioning of the Service. These include: patch management, change control procedures, QA testing prior to release, ACID compliant databases, and logging of all changes to production systems for the Service.

(d) Data confidentiality. Airship has implemented measures to encrypt data in-transit, and at-rest. In addition, Airship uses data pseudonymisation as needed to comply with customer requirements and regulations.

(e) In-Application Security. Robust application security measures Airship offers include Multi-Factor Authentication (MFA), Single Sign-On (SSO), Role Based Access Control (RBAC), configurable password complexity, segregation of duties, logical separation of customer data, and exportable event logs.

Airship recognizes the importance of software supply chain security and takes steps to verify the integrity and security of third-party components and dependencies.

6. Operational Security

(a) Redundancy. Airship infrastructure systems are designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. To provide this redundancy, Airship uses dual circuits, switches, networks and other necessary components. Airship leverages Infrastructure as Code (IaC) practices for consistent and secure provisioning and management of infrastructure, with appropriate security controls applied to IaC pipelines and repositories.

(b) Server Operating Systems. Airship servers use Server Operating System based implementation customized for the application environment. Industry best practice hardening standards, including CIS benchmarks, are used. Data in the Service's production environment is stored using whole disk AES256.

(c) Business Continuity. Airship replicates critical data over multiple systems and locations to help protect against accidental destruction or loss of data in the Service. Airship has established a baseline RPO and RTO, which is available upon request with a signed NDA. At least on a daily basis, Airship backs up to a separate cloud region from the region used for the Service production servers. Replicated data is stored at rest in AES256 encrypted format. Airship has formal documented recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit,

support group unit, application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations, and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable. Airship has implemented and regularly tests its business continuity planning/disaster recovery programs.

(d) Vulnerability Management. Airship Infrastructure as a Service (IaaS) and Operating Systems (OS) are scanned regularly for vulnerabilities, in conformance with Airship's security policies and industry standards. Patch Management processes are in place to respond to and remediate findings from Airship managed scanning, 3rd party testing, and the public Bug Bounty Program. Patching is performed in a timely manner in conformance with Airship's security policies and industry standards.

7. Customer Data

(a) Data Storage and Separation. Customer Data is stored in a multi-tenant environment on public cloud servers. Airship logically separates Customer Data in the Service and conducts tests at least annually to confirm logical separation.

(b) Data minimization. Airship makes available to Customers via the Service capabilities to determine the types of data to be collected based on the processing purposes defined by the Customer. These capabilities include the option to disable data collection in order to prevent collection of any data (with the exception of the data collection opt-in status). In addition, Airship will keep data only as long as necessary in accordance with the Airship Data Retention Schedule.

(c) Data Retention and Deletion. Airship makes available data deletion functionalities directly in the Airship API. Airship will delete all Customer Data in the Service production servers 90 days after termination of Customer's contract. In addition, certain Customer Data stored in Airship Service will be deleted on an ongoing basis in accordance with the Airship Data Retention Schedule. Backup data is stored in AES256 format and deleted in 7 days.

(d) Data Portability. For accounts that do not have Airship's Real-Time Data Streaming (RTDS), Airship makes available to Customers data export functionalities for certain metadata directly in the various Airship API services offering endpoints. For these types of accounts, Airship can provide assistance for more robust data export requests via requests to Airship Support. Accounts with Airship's Real-Time Data Streaming (RTDS) service also have the ability to export more granular data throughout the lifetime of the service. All data exported from Airship API's are in the open-source JSON format. Airship Support can assist with special data export requests (E.g. Legal Holds and Legal Exports).

(e) Localized Data Hosting. By using the Service, Customer consents to storage of Customer Data in the United States or in the European Union, as follows. If the Customer has selected the United States data center location for the Airship Service or Apptimize, all Customer Data stored is located in the United States. If Customer has selected the European Union as the data center location for the Airship Service or Apptimize, all Customer Data is located in the European Union. Live Customer Data is not replicated back

and forth between the EU and US data center data set. Customer Data may be transferred to and accessed from the Airship subsidiaries locations for technical support, error fixes, and other product related services.

(f) Pseudonymization and Encryption. Airship will ensure data is encrypted during transmission to and from the Service. In addition, Airship will keep all data encrypted at rest with Whole Disk Encryption using AES 256 standard. The Service includes additional measures that Customers can configure in order to reduce direct references to persons during processing where it is possible to associate data with a specific person only if additional information is included. Airship has put in place appropriate technical and organizational measures to keep the pseudonymized information separate from the additional information. It is the Customer's responsibility to elect to use these additional measures for pseudonymization of personal data processed in the Service. (g) Restoring data from data loss. Airship has policies and procedures for backups of Customer Data. Airship's relational databases and NoSQL data stores are automatically backed up in a secure fashion on both daily and weekly schedules. Should a data loss event occur, Airship will be able to recover data contained in these backups. Backups are protected using industry best practices.

8. Data Breach Management

If Airship becomes aware of a Data Breach, Airship will notify Customer of the Data Breach within a period not to exceed 48 hours from confirmation of the Data Breach. Airship will take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Breach will be delivered to the email address provided by Customer in the Agreement or in the administration console of the Service. Customer acknowledges that it is solely responsible for ensuring that the contact information set forth in the Agreement (or in the administration console of the Service) is current and valid. Customer agrees that "Data Breaches" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems; or (ii) breach of security of systems outside of Airship's control where Airship is not itself made aware of a data breach.

9. Personnel Security

(a) Background Checks. Airship conducts employee background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

(b) Employee Training. Airship employees are required to (a) execute a confidentiality agreement; (b) undergo annual security training, and (c) if handling Customer Data, complete additional requirements appropriate to their role.

(c) Employee Code of Conduct. Airship employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

10. Privacy by Design

Airship employs Privacy by Design and Privacy by Default principles in its development and operations processes.

11. Authorized Subprocessors

(a) Subprocessor Security. Prior to onboarding subprocessors, Airship conducts a selection process to evaluate the subprocessors' security, privacy, data protection, and confidentiality practices and to assess that subprocessors provide a level of security, data protection, and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Where applicable, Airship enters into data protection agreements providing equivalent obligations as those required from Airship as set forth in the Airship Data Processing Addendum. Subprocessors are re-authorized upon contract renewal or on an annual basis.

(b) Subprocessor List. A current list of Airship's Subprocessors is available here.

12. Security Measures Specific to Generative AI Features of the Airship Service

Airship recognizes the unique security challenges and risks associated with the use of Generative AI technologies. To address these risks, Airship implements the following AI security measures as to the Generative AI functions in the Airship Service:

- Data Security: Airship protects the confidentiality, integrity, and availability of data used for Artificial Intelligence or Machine Learning model ("AI/ML Model") training and inference, including Customer Data and any other proprietary Customer information.
- Model Security: Airship implements measures to protect AI/ML Models from unauthorized access and tampering. This includes secure storage, access controls, and version control for AI/ML Models.
- Robustness and Resilience: Airship designs AI/ML Models to be resilient against adversarial attacks and unexpected inputs. Regular testing and monitoring are performed to ensure AI/ML Model security.
- Bias and Fairness: Airship is committed to mitigating bias and ensuring fairness in AI/ML Models. This includes careful selection of training data, monitoring for bias, and implementing techniques to address any identified biases.
- Privacy: Airship ensures that AI/ML Models are designed and deployed in a privacy-protecting manner, respecting user privacy and complying with applicable data protection regulations.

Additional Standards Specific to Generative AI Function using the Google Gemini/Vertex AI/ML Models:

- Airship leverages the built-in security features provided by Google for the Gemini and Vertex AI/ML Models, such as data encryption, access controls, and privacy-protecting techniques and in accordance with Google AI Principles available at https://ai.google/responsibility/principles/.
- Airship follows Google's best practices for secure AI/ML development and deployment.
- Airship deploys the Google Gemini/Vertex AI AI/ML Models in a privacy-protecting manner, respecting user privacy and complying with applicable data protection regulations. Data generated by these models is held to the same security and compliance standards as other Customer Data in the Airship Service and is audited as such.
- Airship works closely with our third-party AI/ML Models provider, Google, to stay informed about emerging AI security threats and vulnerabilities.

ANNEX III – LIST OF SUB-PROCESSORS

Customer has authorized the use of the following Sub-processors in connection with the Services. The specific Sub-processors and the extent of data Processing and data transfer is based on Customer's configuration and use of the Services and is available at: https://www.airship.com/legal/subprocessors/

Customer may subscribe to receive updates about changes in Sub-processors by visiting https://www.airship.com/legal/subprocessors/.