AIRSHIP DATA PROCESSING ADDENDUM (Revised September 2021) – Previous Version

This Data Processing Addendum ("Addendum") forms part of the Master Subscription Agreement or the online Terms of Subscription Service (the "Agreement") between the customer that has executed this Addendum here and is an Airship customer on the date this Addendum is fully executed ("Customer") and Airship. This Addendum reflects the parties' agreement with regard 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 Addendum 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 Addendum 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 Addendum 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, Airship UK Limited, a company registered in England and Wales, 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. Airship, including its Affiliates, is the Data Processor with respect to Customer Data under EU 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, as amended (the “CCPA”) and other similar state legislation as may be applicable; (iii) the data protection or privacy laws of the United Kingdom; 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 Addendum, 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).

“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 Addendum, 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 his/her specific data subject rights under the 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-overview.

“Service” means, to the extent specified in the applicable Order Form, (1) the Airship Customer Engagement Platform, including the Airship SDKs and APIs, and programs, features, functions, developer tools, report formats and any updates or upgrades of any of the foregoing made generally available by Airship (“Airship Service”), and (2) the Apptimize Testing Platform, including the Apptimize SDKs and APIs, and programs, features, functions, developer tools, report formats and any updates or upgrades of any of the foregoing made generally available by Airship (“Apptimize Service”).

“Standard Contractual Clauses” 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 attached hereto as Annex 1. In case of any transfers of Personal Data under this DPA under the Standard Contractual Clauses from the United Kingdom, the Standard Contractual Clauses shall refer to the European Commission’s decision of 5 February 2010 on Standard Contractual Clauses 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 attached hereto as Annex 2.

“Sub-processor” means any Data Processor engaged by Airship to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this Addendum.

The terms, “Member State”, and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

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 will process Customer Data only as a Data Processor acting on the instructions of Customer.

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 to allow Customer Data to be collected, processed, stored, used, transmitted and disclosed in the manner contemplated by the Agreement and this Addendum, and (iv) 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 accuracy, quality, and legality of Customer Data and the means by which Customer acquires and uses Customer Data.

2.3 Airship's Processing of Customer Data. Airship shall only process Customer Data on behalf of and in accordance with Customer's instructions 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. 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 the GDPR.

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.B to the Standard Contractual Clauses.

The types of Customer Data transmitted are described in detail in Annex I.B to the Standard Contractual Clauses, and may include:

- Customer and Account Users: Account User's login credentials to the Service;
- End Users: Customer may process Personal Data via the Service, the extent of which is determined by Customer based on Customer's configuration and use of the Service, which may include, at Customer's sole discretion and based on the Service package subscribed by the Customer, but is not limited to the following categories of Personal Data: Push tokens, names, mobile phone numbers (if data exporter uses the SMS/MMS notification channel), email addresses (if Customer uses the email notification channel), online identifiers, and location data (if Customer's order includes the location feature).

- Special classes of data. Unless explicitly agreed and stated in the Annex I.B to the Standard Contractual Clauses, Customer is contractually prohibited from processing via the Service any "special categories of data" as defined in Data Protection Laws as well as any Prohibited Data.

3. RIGHTS OF DATA SUBJECTS AND COOPERATION

3.1 Data Subject Requests. Airship will comply fully with the requirements of 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. 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 Addendum. 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 Addendum.

3.3 Government or Other Public Authority Requests. Airship will comply fully with the requirements of Clause 14 and Clause 15 of the Standard Contractual Clauses. If any government agency or body sends Airship a demand for Customer Data (for example, through a subpoena or court order), Airship will attempt to redirect the government agency or body to request that data directly from Customer. As part of this effort, Airship will follow the Airship Policy on Response to Public Authority Requests for Personal Data.

4. AIRSHIP PERSONNEL

In compliance with Clause 8.6 of the Standard Contractual Clauses, 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.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. In connection with Clause 9 of the Standard Contractual Clauses, 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 into a written agreement with each Sub-processor containing data protection obligations not less protective than those described in this Addendum with respect to the protection of Customer Data to the extent applicable to the nature of the Service provided by such Sub-processor. Airship shall make available to Customer the current list of Sub-processors for the Service in Annex III to the Standard Contractual Clauses and by posting that list online at: https://www.airship.com/legal/subprocessors. Customer may subscribe to receive automated notifications of pending changes in Sub-processors at the link in the preceding sentence.

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 and as set forth in detail in Annex II to the Standard Contractual Clauses. 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 Addendum, 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 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 Addendum 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 Addendum; (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 in compliance with Clause 8.6(c) and 8.6(d) of the Standard Contractual Clauses.

8. DELETION OF CUSTOMER DATA

In compliance with Clause 8.5 of the Standard Contractual Clauses, (i) 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; or (ii) if 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. Customer authorizes Airship and its Sub-processors to transfer Customer Data across international borders, including from the EEA 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 Standard Contractual Clauses. To the extent that any Customer Data originating in the EEA 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 Standard Contractual Clauses attached hereto as Annex 1. For the purposes of Annex 1, the Customer shall be deemed to be the "data exporter" and Airship shall be deemed to be the "data importer". The parties agree that: (i) the audits described in Clause 8.9 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with Section 6.4 of this Addendum; and (ii) pursuant to Clause 9 of the Standard Contractual Clauses, Airship may engage new Sub-processors in accordance with Section 5 of this Addendum; and (iii) the certification of deletion referenced in Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses shall

be provided only upon Customer's written request. Each party's signature to the Addendum shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

9.3 Data Transfers from the UK under the Standard Contractual Clauses. In case of any transfers of Personal Data under this DPA under the Standard Contractual Clauses from the United Kingdom, to the extent such transfers are subject to Data Protection Laws applicable in the United Kingdom ("UK Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 shall hereby be deemed to have the same meaning as the equivalent reference in the UK Data Protection Laws; (ii) References in the Standard Contractual Clauses to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom"; and (iii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter is established shall hereby be deemed to refer to an obligation under UK Data Protection Laws. The parties agree that the terms of the transfer shall be governed by the Standard Contractual Clauses attached hereto as Annex 2. For the purposes of Annex 2, the Customer shall be deemed to be the "data exporter" and Airship shall be deemed to be the "data importer". The parties agree that: (i) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Section 6.4 of this Addendum; (ii) pursuant to Clause 5(h) and Clause 11 of the Standard Contractual Clauses, Airship may engage new Sub-processors in accordance with Section 5 of this Addendum; and (iii) the Sub-processor agreements referenced in Clause 5(j) and certification of deletion referenced in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Customer's written request. Each party's signature to the Addendum shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

9.4 Amendments to Address Changes in Data Protection Laws. Notwithstanding anything to the contrary, this Section 9 and Annex 1 (including its appendices) may be amended by Airship to address changes in Data Protection Laws with fifteen (15) days' notice to Customer.

9.5 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 9.5 (Legacy Standard Contractual Clauses). This Section 9.5 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 sell any such personal information. 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. The terms “business,” “personal information,” “service provider,” “sale,” and “sell” are as defined in Section 1798.140 of 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 Addendum 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 Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement, this Addendum will prevail to the extent of that conflict.

11.2 Claims. Any claims brought under or in connection with this Addendum 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 Addendum, 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 Addendum, its successors and permitted assignees will have any right to enforce any of its terms. Any claims against Airship or its Affiliates under this Addendum 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 Addendum 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 Addendum 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 Addendum shall only become legally binding between Customer and Airship when executed as described in the introductory paragraphs to this Addendum.

Annex 1 – Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the

extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or

pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to

notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) days in advance, thereby giving the

data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data

exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including

remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied

during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the

data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name:

   Address:

   Contact person's name, position and contact details:

   Activities relevant to the data transferred under these Clauses: Customer engagement platform for marketing to and communicating with Data Exporter's end users / consumers.

   Signature: _____

   Date: _____

   Role (controller/processor): Data Controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Airship Group, Inc.

   Address: 1225 W. Burnside, Suite 401, Portland, OR 97209

   Contact person's name, position and contact details: Scott Allen, CFO, scott.allen@airshp.com

Activities relevant to the data transferred under these Clauses: Customer engagement platform for marketing to and communicating with Data Exporter's end users / consumers.

Signature: _____

Date: _____

Role (controller/processor): Data Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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 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").

Categories of personal data transferred:

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

End Users: Data Exporter may process Personal Data via the Services, the extent of which is determined by Data Exporter based on Data Exporter's configuration and use of the Services, which may include, in Data Exporter's sole discretion based on the Service package subscribed to by Data Exporter, the following categories of Personal Data: push tokens, names, mobile phone numbers (if data exporter uses the SMS/MMS notification channel), email addresses (if Customer uses the email notification channel), online identifiers, and location data (if Customer's use includes the location feature).

Sensitive data transferred.

Data exporter 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.

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

Ongoing during the term of the Agreement.

Nature of the processing

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

Purpose(s) of the data transfer and further processing

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

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/.

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/.

C. COMPETENT SUPERVISORY AUTHORITY

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

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.

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 Customer Engagement Platform ("CEP"), the Apptimize Testing Platform ("Apptimize"), and any other services or functionalities related to either the CEP 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.

2. Information Security Program and Attestations

Airship maintains an information security program that includes the adoption and enforcement of internal policies and procedures and 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 CEP (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.

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.

(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.

5**. Application Security**

(a) Software Development. Airship employs a static code review process to increase the security of the code used to provide the Service. This code is reviewed and approved based on peer review prior to staging the code. All development for the Service is based on Secure Development Lifecycle (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 SOC 2 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.

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.

(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 implemented and regularly tests its business continuity planning/disaster recovery programs.

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 CEP 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 CEP 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 CEP 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'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.

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.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors listed online at https://www.airship.com/legal/subprocessors/ in connection with the Services. The specific sub-processors and the extent of data transfer is based on Data Exporter's configuration and use of the Services.

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

Annex 2 – Standard Contractual Clauses (February 5, 2010 version for purposes of UK transfers)

INTRODUCTION

Both parties have agreed on the following Contractual clauses (the "**clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in appendix 1.

AGREED TERMS

1. Definitions

For the purposes of the clauses:

(a) "**personal data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) the "**data exporter**" means the controller who transfers the personal data;

(c) the "**data importer**" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) the "**sub-processor**" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the clauses and the terms of the written subcontract;

(e) the "**applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

(f) "**technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration,

unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in appendix 1 which forms an integral part of the clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this clause, clause4(b) to 4(i), clause 5(a) to 5(e), and 5(g) to 5(j), clause 6.1 and 6.2, clause 7, clause 8.2, and clause 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this clause, clause 5(a) to 5(e) and 5(g), clause 6, clause 7, clause 8.2, and clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this clause, clause 5(a) to 5(e) and 5(g), clause 6, clause 7, clause 8.2 and clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the clauses, with the exception of appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the clauses, unless the clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the clauses; and

(j) that it will ensure compliance with clause 4(a) to 4(i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the clauses; if it cannot provide such compliance for whatever reasons, it

agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i)any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the clauses, or any existing contract for sub-processing, unless the clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in clause 3 or in clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause clause 3 or in clause 11, because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the clauses.

7. Mediation and jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the clauses, the data importer will accept the decision of the data subject:

7.1 to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

7.2 to refer the dispute to the courts in the Member State in which the data exporter is established.

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Co-operation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9. Governing law

The clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the clause.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall

remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the clauses.

11.4 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.5 The data exporter shall keep a list of sub-processing agreements concluded under the clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 To the Standard Contractual Clauses

This Appendix forms part of the clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The entity that signed the Data Processing Addendum to which this Appendix 1 is attached.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Airship Group Inc., a company incorporated in Delaware, Apptimize LLC and any other Affiliate of Airship, in each case to the extent such parties are subject to Section 9.2 of the Addendum. Data importer provides technical support and account management services in connection with the Airship Customer Engagement SaaS platform ("Service") and related services to its customers.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Any individual accessing and/or using the Service through the data exporter's Account as authorized by data exporter ("Account Users"); and any end user of a mobile application, web domains, devices, software applications and/or communication channels owned or controlled by data exporter and to or with respect to whom data exporter sends notifications or processes personal data via the Service (collectively, "End Users").

Categories of data

The personal data transferred concern the following categories of data (please specify):

- Data exporter and Account Users: Account User's login credentials to the Service;
- End Users: Data exporter may process personal data via the Service, the extent of which is determined by data exporter based on data exporter's configuration and use of the Service, which may include, at data exporter's sole discretion based on the Service package subscribed by the data exporter, but is not limited to the following categories of personal data: Push tokens, names, mobile phone numbers (if data exporter uses the SMS/MMS notification channel), email addresses (if data exporter uses the email

notification channel), online identifiers, and location data (if data exporter's order includes the location feature).

Special categories of data

Data exporter is contractually prohibited from processing via the Service any "special categories of data" as defined in Data Protection Laws as well as any individual financial data, credit or debit card numbers, individual health information, or government issued identification numbers.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Data importer provides a subscription to its notification and data platform, as described in the Master Subscription Agreement or the online Terms of Subscription Service entered into between the data exporter and the data importer.

Appendix 2 To the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with clauses 4(d) and 5(c) (or document/legislation attached):

The Data Importer shall implement and maintain technical and organizational security measures as set out in Section 6 of the Data Processing Addendum entered into between the Data Exporter and the Data Importer.