DPA Amendment – New EU Standard Contractual Clauses and UK IDT

Effective Date: December 27, 2022	
Airship Group, Inc. and its Affiliates ("**Airship**")	Customer: Customer entity that has executed an Order Form and DPA with Airship ("**Customer**")
The New SCC Amendment is effective as of the Effective Date above.	
Notice Address: As defined in the DPA	Notice Address: As defined in the DPA

Customer and Airship have entered into either a Data Processing Addendum or a Data Transfer Addendum, (each a and together the "**DPA**"), reflecting 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. The Parties hereby agree to amend the DPA as follows in this DPA Amendment. The DPA otherwise remains in full force and effect.

Capitalized terms not defined herein shall have the meanings given to them in the DPA or the Agreement.

1. **Section 1 Definitions** of the DPA is hereby amended as follows:
   1.1. The following definitions are hereby added to Section 1 of the DPA:

      "**ICO**" means the United Kingdom's Information Commissioner's Office.

      "**UK DPA**" means the International Data Transfer DPA issued by the ICO to the EU Commissions Standard Contractual Clauses VERSION B1.0, in force 21 March 2022 and set forth in Annex 2 to this DPA.

   1.2. The definition of the term "Standard Contractual Clauses" is hereby replaced in its entirety with the following definition: "**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.

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. All references to the Standard Contractual Clauses or to the Privacy Shield framework as a transfer mechanism for personal data from the EU to the US as used in the DPA are hereby amended to refer to the Standard Contractual Clauses in Annex 1 of this DPA Amendment.

3.   **Data Transfers from the UK under the Standard Contractual Clauses.** In case of any transfers of Personal Data under the 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"), the Parties agree that the terms of the transfer shall be governed by the UK DPA. As a result, all references to the Standard Contractual Clauses or to the Privacy Shield framework as a transfer mechanism for personal data from the UK to the US used in the DPA are hereby amended to refer to the UK DPA as follows. The UK DPA is subject to the DPA as further amended by this DPA Amendment, and the Agreement; forms an integral part of this DPA; and reflects the Parties' agreement with respect to the processing of UK Personal Data. The Parties hereby agree to supplement the Annex 1 of this DPA Amendment containing the Standard Contractual Clauses with the UK DPA and any reference to the Standard Contractual Clauses shall refer to the Standard Contractual Clauses together with the UK DPA for the purposes of Personal Data subject to UK Data Protection Laws. For the purposes of the UK DPA, 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 EU SCCs shall be carried out in accordance with the "Audits" Section of the DPA; and (ii) pursuant to Clause 9 of the EU SCCs, Airship may engage new Sub-processors in accordance with the "Sub-Processors" Section of the DPA; and (iii) the certification of deletion referenced in Clause 8.5 and Clause 16(d) of the EU SCCs shall be provided only upon Customer's written request. Each party's signature to the DPA Amendment shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder. If there is any conflict between the UK DPA and the DPA or this DPA Amendment, the UK DPA shall control.

4.   **Entire Agreement.** The terms and conditions herein constitute the entire agreement between the Parties with respect to the subject matter of herein and supersede any previous and contemporaneous agreements and understandings whether oral or written, between the parties hereto with respect to the subject matter hereof.

ANNEX 2A TO DPA: 2021 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 benefiting 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: Customer as identified in the DPA

    Address: Address identified in the DPA

    Contact person's name, position and contact details: As identified in the DPA

    Activities relevant to the data transferred under these Clauses: Airship and/or Apptimize Service(s) for marketing to and communicating with Data Exporter's end users / consumers.

    Signature:

    Date: Dated as of the Effective Date

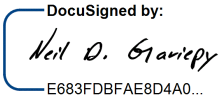   Role (controller/processor): Data Controller

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: Neil Gariepy, VP, Infrastructure and Security, privacy@airship.com

Activities relevant to the data transferred under these Clauses: Airship and/or Apptimize Service(s) for marketing to and communicating with Data Exporter's end users / consumers.

Signature:

DocuSigned by:

Neil D. Graviepy

E683FDBFAE8D4A0...

Date: 12/21/2022

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

If the data exporter is established in an EU Member State: the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority.

If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR): the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority.

If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority.

<u>ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA</u>

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 Service, the Apptimize Service ("Apptimize"), and any other services or functionalities related to either the Services.
"**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 Service (which includes mobile app, email, API, and SMS solutions, and Apptimize) annually for compliance with the SOC 2 Type II availability, confidentiality, and security trust principles. The Third Party Auditor issues a SOC2 Report, which is available to the Customer upon request under signed NDA. The Airship SOC2 Report includes the cloud provider subprocessors used by Airship, but not the other subprocessors.

3. Access Controls
 (a) Data Center Access Controls.

- Leading Cloud Data Centers. Airship uses Cloud Platform (Google Cloud) or for certain Airship customers, depending on location or the Airship services subscribed to, Amazon Web Services (AWS), to provide infrastructure services to host and operate the Service. By using Google Cloud's

Trusted Infrastructure or AWS's Security, Identity, and Compliance Service, Airship is able to take advantage of their sophisticated security environments.

- Physical Access Control. The cloud data centers used to provide the Service are Tier 4 certified, ISO 27001, and SOC 2 Type II certified computing facilities. These cloud data center facilities maintain on-site security operations responsible for all physical data center security functions 24 hours a day, 7 days a week, with CCTV monitoring and access controls. The CCTV monitoring footage is kept for 90 days.

(b) Logical and Data Access Controls.

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

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

- *Internal Data Access Processes and Policies.* Airship's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process data in the Service.
- *Access Management.* Airship employs a centralized access management system to control personnel access to production servers for the Service to a limited number of authorized personnel. Central network-based authentication systems are designed to provide Airship with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information for the Service. Airship requires the use of unique user IDs, strong passwords, two factor authentication and access lists for Airship personnel to access the Service. Airship personnel are granted access rights to the Service based on: (i) the authorized personnel's job responsibilities; (ii) job duty requirements necessary to perform authorized tasks based on least privilege; and (iii) a need to know basis. The granting or modification of access rights must be performed in accordance with Airship's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Log-ins to the Service are logged into the Security Information and Event Management system (SIEM).
- *Access Controls.* Security events for the Service, including login failures, use of privileged accounts, changes to access models or file permissions, modifications to installed software or operating systems, changes to user permissions or privileges are logged on the relevant systems. Logs are generated through monitoring and alerting systems, and are held from 30 days to 1 year, depending on the system.

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:

v.05.2022 Amendment New SCC and UK IDT

- 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 Service will be deleted on an ongoing basis in accordance with the Airship Data Retention Schedule. Backup data is stored in AES256 format and deleted in 7 days.

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

(e) Localized Data Hosting. By using the Service, Customer consents to storage of Customer Data in the United States or in the European Union, as follows. If the Customer has selected the United States data center location for the Airship Service or Apptimize, all Customer Data stored is located in the United States. If Customer has selected the European Union as the data center location for the Airship Service or Apptimize, all Customer Data is located in the European Union. Live Customer Data is not replicated back and forth between the EU and US data center data set. Customer Data may be transferred to and accessed from the Airship subsidiaries locations for technical support, error fixes, and other product related services.

(f) Pseudonymization and Encryption. Airship will ensure data is encrypted during transmission to and from the Service. In addition, Airship will keep all data encrypted at rest with Whole Disk Encryption using AES 256 standard. The Service includes additional measures that Customers can configure in order to reduce direct references to persons during processing where it is possible to associate data with a specific person only if additional information is included. Airship has put in place appropriate technical and organizational measures to keep the pseudonymized information separate from the additional information. It is the Customer's responsibility to elect to use these additional measures for pseudonymization of personal data processed in the Service.

(g) Restoring data from data loss. Airship'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.

<u>ANNEX III – LIST OF SUB-PROCESSORS</u>

The controller has authorised the use of the following sub-processors 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, and as described at https://www.airship.com/legal/subprocessors/.

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

ANNEX 2B TO DPA

UK ADDENDUM

This UK Addendum to the DPA is executed upon the date of the last signature ("UK Addendum Effective Date") by Airship and the Customer identified below in Table 1 of this UK Addendum amending the DPA pursuant to the Agreement governing the use of the Airship Services by Customer. The Parties agree to supplement Annex I to the DPA containing the EU Standard Contractual Clauses with the enclosed UK Addendum in accordance with Section 9.3 of the DPA.

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start Date	Upon the UK Addendum Effective Date.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)

Parties' details	Customer (See signature section for further details)	Airship Group, Inc. (See signature section for further details)
Key Contact	Full Name (optional): As indicated in the DPA Job Title: As indicated in the DPA Contact details including email: As indicated in the DPA	Full Name (optional): Neil Gariepy Job Title: VP, Infrastructure and Security Contact details including email: privacy@airship.com
Signature (if required for the purposes of Section 2)	See signature section of the DPA for further details	See signature section of the DPA for further details

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: As set forth in Annex 1 to this DPA Reference (if any): As set forth in Annex 1 to this DPA Other identifier (if any):

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As per Table 1 above.
Annex 1B: Description of Transfer: As provided in Annex I to the Standard Contractual Clauses included in this DPA.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

The Data Importer shall implement and maintain technical and organizational security measures as set out in Annex 2 to the EU SCCs entered into between the Data Exporter and the Data Importer.

Annex III: List of Sub processors (Modules 2 and 3 only):

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/ .

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19:
	Importer
	Exporter
	✓neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum

will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

　　a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's

       processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

       "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.