GDPR PERSONAL DATA PROCESSING ADDENDUM

This GDPR Personal Data Processing Addendum (the "**Agreement**" or "**DPA**"), by and between **Airlines Reporting Corporation**, a U.S. corporation registered in the State of Delaware with its principal place of business at 3000 Wilson Blvd., Arlington, VA 22201 (the "**Processor**" or "**ARC**"), and any airline customer of ARC on whose behalf ARC processes Personal Data (the "**Controller**" or "**Customer**") pursuant to 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, repealing Directive 95/46/EC (General Data Protection Regulation) (the "**GDPR**") forms part of, and is subject to, the primary agreement for products and/or services (collectively, the "**Services**") between ARC and Customer (the "**Primary Agreement**"). This DPA shall take effect only upon reasonable prior written notice from ARC to Customer providing Customer with an opportunity to object. Notwithstanding the foregoing, this DPA shall only apply to the extent ARC and Controller have not separately executed a signed data processing agreement/addendum related to GDPR. This DPA includes the Standard Contractual Clauses (SCC) in Schedule 4 hereto; any updates or revisions to the SCC required by applicable law shall be automatically incorporated by reference herein.

The Controller and the Processor shall jointly be referred to as the "**Parties**" and individually as a "**Party**".

WHEREAS:

(A) The Controller is the controller (within the meaning of the GDPR, as defined in Clause 1.1 below) of the personal data set out in Schedule 1 (Personal Data) to this Agreement (the "Personal Data").

(B) The Processor is located exclusively within the United States and does not offer goods or services to Personal Data subjects in the European Union, and does not monitor the behaviour of Personal Data subjects that takes place within the European Union.

(C) The Controller intends to transfer the Personal Data to the Processor, and the Processor intends to accept the Personal Data transferred to it, for processing on behalf of the Controller, in accordance with this Agreement and regulations pertaining to personal data processing, binding both the Processor and the Controller.

IT IS AGREED as follows:

1. PURPOSE

1.1 The Controller may entrust the Processor with processing the Personal Data on behalf of the Controller, on terms set out in this Agreement and applicable regulations pertaining to the processing of personal data – in particular the GDPR.

1.2 The type of Personal Data and categories of the Personal Data subjects, as well as the subject -matter, duration, nature and purpose of the processing are set out in Schedule 1 (*Personal Data*) to this Agreement.

1.3 The Parties undertake to perform the obligations set out in this Agreement with the highest degree of professional diligence in order to legally, organisationally and technically secure the Parties' interests, as well as the interests of the Personal Data subjects, with respect to the processing of the Personal Data.

2. REPRESENTATIONS OF THE PROCESSOR

The Processor represents that it:

(a) implemented technical and organisational measures ensuring the processing the Personal Data in accordance with applicable regulations, in a manner ensuring the protection of the rights of the Personal Data subjects (a list of technical and organisational measures is set out in Schedule 2 (Technical and Organisational Measures) to this Agreement); and

(b) possesses reasonably proper means, experience, expertise and properly trained staff, enabling it to process the Personal Data in the scope and for the purpose set out in this Agreement.

3. PROCESSING PERSONAL DATA

General rules of processing

3.1 Subject to Clause 3.2 below, the Processor shall process the Personal Data in accordance with the terms of this Agreement or pursuant to separate written instructions from the Controller (including by way of electronic mail).

3.2 The Processor may process the Personal Data if it is required to do so by law of the European Union or a Member State law to which the Processor is subject. In such a case, the Processor must inform the Controller of such legal requirement at least 24 (twenty-four) hours in advance of commencing such processing (unless prohibited by law for reasons of protecting the public interest).

3.3 Processing the Personal Data by the Processor is limited to the purpose and scope set out in Schedule 1 (*Personal Data*) to this Agreement.

3.4 The Processor must maintain a record of its processing activities, comprising information required by applicable regulations, unless applicable regulations exempt it from maintaining such a record.

3.5 The Processor must maintain a record of all categories of processing activities carried out on behalf of the Controller, in accordance with Article 30 section 2 of the GDPR, unless applicable regulations exempt it from maintaining such a record.

3.6 Any Personal Data processing operations requested by the Controller shall be performed by the Processor promptly, in particular if the request pertains to erasing Personal Data pursuant to a demand by a Personal Data subject.

3.7 Taking into account the nature of the processing of the Personal Data, the Processor shall assist the Controller in fulfilling the Controller's obligation to respond to requests for exercising the Personal Data subject's rights in accordance with applicable regulations, by implementing appropriate technical and organisational measures.

Authorisation to Process

3.8 The Processor shall ensure that persons involved in Personal Data processing operations in its organisation:

(a) receive written authorisations to process the Personal Data;

(b) are familiar with applicable regulations pertaining to personal data processing (including any amendments) and liability for infringement;

(c) process the Personal Data exclusively upon the Controller's instructions (save as permitted under Clause 3.2 above); and

(d) undertake to keep the Personal Data and any security measures implemented by the Processor confidential in perpetuity, unless they are under an appropriate statutory obligation of confidentiality.

3.9 The Processor shall maintain a record of issued authorisations to process the Personal Data, referred to in Clause 3.8 (a) above.

Engaging Sub-Processors

3.10 The Processor may sub-contract the processing of the Personal Data to a sub-processor provided that, prior to transferring any Personal Data to a sub-processor, it:

(a) obtains the Controller's written consent (including by way of electronic mail);

(b) concludes an agreement with the sub-processor for processing Personal Data containing the same data protection obligations as set out in this Agreement; and

(c) ascertains that the sub-processor provides sufficient guarantees of implementation of proper technical and organisational measures, so that its processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject.

3.11 In case the sub-processor fails to fulfil its obligations of Personal Data protection, the Processor shall be fully liable towards the Controller for fulfilment of the sub-processor's obligations.

3.12 The list of sub-processors approved by the Controller as of the date of this Agreement is set out in Schedule 3 (*Approved Sub-Processors*) to this Agreement.

4. PERSONAL DATA SECURITY

Security Measures

4.1 The Processor shall use technical and organisational measures which are appropriate to the threats and nature, scope, context and purposes of processing of the Personal Data, assuring security of the Personal Data, in particular from their accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

4.2 A list of security measures to be used by the Processor in relation to the processing of the Personal Data constitutes Schedule 2 (*Technical and Organizational Measures*) to this Agreement.

4.3 The Processor shall regularly monitor the state of the implemented measures of security of the Personal Data, as well as existing security threats, and (if required) update the used technical and organisational measures, in order to assure reasonable Personal Data protection.

Cooperation Regarding Security

4.4 The Processor shall, taking into account the nature of processing of the Personal Data and the information available to the Processor, assist the Controller in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR.

4.5 The Processor shall, prior to taking any actions, promptly notify the Controller of any case of:

(a) any authority demanding that the Personal Data be made available to it, unless it is prohibited to disclose that information by applicable regulations, duties of confidence or other legal restriction;

(b) any Personal Data subject issuing a Data Subject Access Request pertaining to the processing of the Personal Data or its contents by the Processor.

4.6 The Processor shall promptly, in any case not later than within 48 (forty-eight) hours of detection, notify the Controller of any detected Personal Data breaches, providing the Controller with any information pertaining to the breach which is available to the Processor, in particular regarding:

(a) the nature of the Personal Data breach, including, where possible, the categories and approximate number of Personal Data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained

(c) the likely consequences of the Personal Data breach; and

(d) the measures taken or proposed to be taken by the Processor to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.7 The Processor shall cooperate with the Controller, in order to identify details of the Personal Data breach notified to the Controller, in particular its causes and results of its occurrence, as well as implement measures advised by the Controller, aiming to mitigate possible adverse effects of the Personal Data breach, and remedial actions.

4.8 The Processor shall promptly inform the Controller if, in its opinion, any instructions received from the Controller infringes applicable regulations or other legal obligation.

5. COOPERATION

5.1 The Processor is obliged to cooperate with the Controller or the auditor engaged by the Controller during the ongoing control proceedings, in a manner enabling the Controller to confirm that the Processor has properly carried out its obligations.

5.2 Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

6. TERMINATION

6.1 This Agreement enters into force on the date of its signing and remains in force until the termination and/or expiry of the last agreement binding the Parties, which give basis for the necessity of processing of the Personal Data by the Processor.

6.2 Upon the Processor breaching any of its obligations set out in this Agreement, the Controller may terminate, with immediate effect, any agreement which gives basis for the necessity of processing of the Personal Data by the Processor.

6.3 Not later than on the date of termination of this Agreement the Processor shall:

(a) delete all Personal Data; or

(b) return to the Controller all carriers containing the Personal Data and delete all existing copies of the Personal Data, unless Union or Member State law requires further storage of a part of or all the Personal Data by the Processor,

depending on the Controller's choice communicated to the Processor in writing (including by way of electronic mail) at least 7 (seven) days before the date of termination of this Agreement.

6.4 In case of terminating of this Agreement pursuant to Clause 6.2 above, the Controller's choice shall be communicated to the Processor in the immediate termination notice.

6.5 The Actions set out in Clause 6.3 above shall be documented in a written protocol signed by a representative of the Processor and delivered to the Controller within 7 (seven) days of the performance of the actions described therein.

7. LIABILITY

7.1 The Processor shall be liable for any damage resulting directly or indirectly from processing the Personal Data if it (i) failed to fulfil its obligations under this Agreement or (ii) it acted outside (or contrary to) the instructions of the Controller.

8. NOTICES

8.1 Any correspondence between the Parties in relation to this Agreement will be prepared in writing, in English, and will be deemed delivered:

(a) with the moment of delivery – in case of personal delivery or with the moment of receipt – in case of postage (registered mail with a confirmation of receipt) or delivery via a reputable courier service; or

(b) in case of correspondence via email, the date and time at which the email was delivered.

8.2 The Parties appoint their representatives authorised to receive deliveries referred to in Clause 8.1 above. Any correspondence will be sent to the relevant address indicated below or to another address communicated by the other Party in writing in accordance with this Agreement:

(a) to the Controller:

as stated in Controller's public privacy policy.

(b) to the Processor:

Airlines Reporting Corporation
3000 Wilson Blvd., Suite 300, Arlington, VA 22201
attention: Data Protection Officer
email: privacy@arccorp.com
with copy to: legalteam@arccorp.com

8.3 The Parties shall inform their representatives indicated in Clause 8.2 above of transferring their personal data to the other Party, providing them with any information required by applicable regulations, in particular information about their rights and about the fact that the transfer of their personal data was effected pursuant to this Agreement, for the purpose of performing its provisions.

9. FINAL PROVISIONS

Remuneration

9.1 The Processor is not entitled to a remuneration for performing this Agreement.

Entire Agreement

9.2 Agreement constitutes the whole agreement between the Parties and replaces in full any previous or simultaneous arrangements made by the Parties (in writing or orally) in the scope regulated by this Agreement.

Schedules

9.3 Schedules to this Agreement constitute an integral part of this Agreement and shall be construed jointly with the main text of this Agreement.

Governing Law

9.4 Agreement shall be governed by, and construed in accordance with, the laws of the EU Member State where the Controller is based. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales; or (iii) where the Agreement is governed by the laws of Switzerland, the laws of Switzerland.

Dispute Resolution

9.5 Any disputes between the Parties shall be resolved in amicable negotiations. In case the Parties do not reach an agreement within 30 (thirty) days of the date of notifying the dispute to the other Party, the dispute will be directed for resolution to a common court relevant for the registered office of the Controller.

Assignment

9.6 No Party shall be entitled to assign any of its rights and/or obligations under this Agreement without the prior written consent of the other Party.

Amendments

9.7 Any amendment to this Agreement proposed by ARC must be in writing and must be provided to the Controller with reasonable written notice and an opportunity to object prior to taking effect. Any amendment to this Agreement proposed by the Controller must be in writing and must be agreed upon in writing by ARC, otherwise being null and void.

SCHEDULE 1
Personal Data

While the exact type, categories, and scope of Personal Data to be processed by ARC on behalf of Customer will depend on the nature and content of the specific Primary Agreement between the Parties, they may generally involve the following:

<table>
<tr>
<td>Type of Personal Data

(e.g. name, surname, address, personal identification number, telephone number, email, location data, IP address)</td>
<td>Airline passengers and/or purchasers of airline tickets:
1. First and last name
2. Credit card number and related information necessary to process credit card payment.
3. Passenger Name Record (PNR) reference
4. Ticket/document number
5. Date of birth (required when the age of the passenger is used to determine the applicability of a fare or a tax/fee/charge.)
6. Client/customer identification: a code assigned by an agency or airline to identify the customer
7. Frequent Flyer Reference Number
8. Order ID (uniquely identifies the record of agreement of one party with another to receive products and services under specified terms and conditions.)
9. Passenger-specific data (travel agency- or Controller-specified information associated to the passenger).
10. Passenger type code (required when it is used to determine the applicability of a fare or a tax/fee/charge):

<table>
<tr><th>Value</th><th>Definitions</th></tr>
<tr><td>CA</td><td>Cargo Attendant (international only)</td></tr>
<tr><td>CD</td><td>Senior Citizen</td></tr>
<tr><td>CH</td><td>Child</td></tr>
<tr><td>CL</td><td>Clergy/Missionary</td></tr>
<tr><td>CP</td><td>Companion Passenger Traveling with a Fare paying Passenger</td></tr>
<tr><td>DG</td><td>Government, Diplomatic, or specified category of Persons/Nationals traveling at a Government ordered fare</td></tr>
<tr><td>EM</td><td>Emigrant (international only)</td></tr>
<tr><td>IE</td><td>Escort to accompany an Inadmissible Passenger</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>IN</td><td>Infant</td></tr>
<tr><td>JC</td><td>Job Corps</td></tr>
<tr><td>LA</td><td>Labor Discount (international only)</td></tr>
<tr><td>M</td><td>Military Reserved Fare</td></tr>
<tr><td>MA</td><td>Military Category A</td></tr>
<tr><td>MR</td><td>Military Recruit</td></tr>
<tr><td>MU</td><td>Military Standby Fare</td></tr>
<tr><td>MZ</td><td>Military Category Z</td></tr>
<tr><td>PG</td><td>Pilgrim Fare (international only)</td></tr>
<tr><td>SC</td><td>Ship Crew--Individual</td></tr>
<tr><td>SD</td><td>Student Fare (international only)</td></tr>
<tr><td>TD</td><td>Teacher Discount (international only)</td></tr>
<tr><td>Z</td><td>Youth Reservation Fare</td></tr>
</table>

Travel agency personnel: first and last names, email address
</td></tr>
<tr><td>Categories of the Personal Data subjects

(e.g. employees, contractors, business partners, clients, distributors)</td><td>Customers of Controller who purchase tickets through travel agencies with a point-of-sale in the United States, for air travel with Controller.

Owners and employees of aforementioned travel agencies.</td></tr>
<tr><td>Scope of Personal Data Processing

(operations made on the conveyed Personal Data, e.g. collecting, recording, organising, structuring, adapting, storing, altering, retrieving using, disclosing, combining, erasing)</td><td>Financial settlement of ticket transactions between Controller and travel agencies using ARC’s clearinghouse services and analysis for development of aggregated, anonymized data products/services, i.e., collecting, recording, organising, structuring, adapting, storing, altering, retrieving, using, analysing, disclosing, combining, erasing.</td></tr>
<tr><td>Nature of the Processing

(e.g. systematic / occasional)</td><td>systematic</td></tr>
</table>

Purpose of Processing (e.g. performing the agreement dated..., personnel management, task management, workplace monitoring, organising deliveries, HR)	performing the Primary Agreement, which may be the Carrier Services Agreement (the "CSA"), including the Direct Connect Supplementary Agreement, as applicable.
Duration of Processing (e.g. duration of the agreement dated...)	duration of the Primary Agreement.

SCHEDULE 2

Technical and Organisational Measures

When Processing Personal Data on behalf of Customer in connection with the Services, Processor shall ensure that it implements and maintains compliance with appropriate technical and organizational security measures for the Processing of such data. Accordingly, Processor has and will continue to implement the following measures:

1. Written Information Security Program (ISP) Policy
2. Communications and Operations Management Policy to ensure that information processing and communications facilities are used and operating in a defined and secure manner (requirements for creation of data centers and office locations, segregation of duties in business technology activities, etc.)
3. Risk Assessment Procedure Policy (threat and vulnerability assessments, risk rating, etc.)
4. Written Security Management Plan Policy (Asset List, Risk Assessment Process, Responsibilities of Management Personnel, etc.)
5. Certifications: PCI-DSS and ISO 27001
6. Encryption of all sensitive information, including Personal Data and credit card numbers according to PCI.
7. Written Encryption Key Management Policy.
8. Written Enterprise Logging and Monitoring Policy for ARC networks and information systems to detect deviations from security policy and unauthorized activities.
9. Written Incident Response Team Policy
10. Written Mobile Portable Storage Device Policy
11. Access controls
    a. Written User Credential Standard Policy (username and password requirements).
    b. Written Physical Security Policy (badging, secure placement of equipment, cameras/surveillance, etc.)
    c. Written User Access Control and Management Policy (privileged access for administrators, two-factor authentication for telework, etc.)
12. Written Network Security Policy
13. Written Vulnerability Scanning Mitigation Policy to identify potential security weaknesses that may pose threats to the confidentiality, integrity and availability of ARC network devices (e.g., routers, switches), security devices (i.e., firewalls, Vulnerability Management Project server, IDS/IPS), and servers (e.g., UNIX and Windows-based systems).
14. Written Patch Management Policy (Oracle, Cisco, Windows and Linux)
15. Written Penetration Testing Scanning and Mitigation Policy) (processes for regularly testing, assessing, and evaluating the effectiveness of Technical and Organizational Measures to ensure the security of the processing)
16. Wireless Communications Policy (access requirements)
17. Written Records Management Policy (records creation and management, legal holds, retention schedule, security, disposal, and responsibilities of data stewards, owners, etc.)
18. Written Data Classification Policy (list of classifications, identification of data owners, stewards, custodians, and users, guidance matrix on determination and labelling, etc.)
19. Written Operational Incident Policy (incident reporting requirements, critical security control system failures, etc.).
20. Written Backup Retention Policy (ensures that Personal Data is protected against accidental destruction or loss; back-ups are taken on a regular basis; back-ups are encrypted and are secured; documented and regularly tested failover procedures are in place.)

Controller may request additional measures, in accordance with the requirements of the GDPR, in particular when they are derived from the recommendations of the GDPR supervising authorities.

SCHEDULE 3
Approved Sub-Processors

No.	Name	Address
1.	Amazon Web Services	410 Terry Avenue North, Seattle, WA 98109-5210, USA
2.	Ensono LP	3333 Finley Rd, Downers Grove, IL 60515, USA
3.	SalesForce	415 Mission St, San Francisco, CA 94105, USA
4.	Snowflake Inc.	450 Concar Drive, San Mateo, CA 94402, USA
5.	11:11 Systems	695 Route 46, Suite 301 Fairfield, NJ 07004, USA

SCHEDULE 4

Standard Contractual Clauses (CONTROLLER TO PROCESSOR)

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)1 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 organizational 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 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 Union4 (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 noncompliance. 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 subprocessors at least seven (7) business 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 subprocessor 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 subprocessor 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 sub-processor) 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 safeguards12;

(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 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the jurisdiction applicable per Section 9.4 of the Agreement.

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 jurisdiction applicable per Section 9.4 of the Agreement.

(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.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: the Customer that is Party to this DPA

Address: as stated in Customer's public privacy policy or as otherwise communicated to ARC in writing.

Contact person's name, position and contact details: as stated in Customer's public privacy policy or as otherwise communicated to ARC in writing.

Activities relevant to the data transferred under these Clauses: as specified in the Agreement.

Role: Controller

Data importer(s):

1. Name: Airlines Reporting Corporation

Address: 3000 Wilson Blvd., Suite 300, Arlington, VA 22201

Contact person's name, position and contact details: Data Protection Officer, (703) 816-8000, privacy@arccorp.com

Activities relevant to the data transferred under these Clauses: as specified in the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

AS SPECIFIED IN SCHEDULE 1 (SEE ABOVE)

C. COMPETENT SUPERVISORY AUTHORITY

a) Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

b) Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

c) Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the Data Protection Commission of Ireland, available per the following contact information, shall act as competent supervisory authority: 21 Fitzwilliam Square, D02 RD28 Dublin 2, Tel. +353 76 110 4800, Email: info@dataprotection.ie.

d) Where Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws and Regulations"), the Information Commissioner's Office ("ICO") shall act as competent supervisory authority.

e) Where Customer is established in Switzerland or falls within the territorial scope of application of the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws and Regulations"), the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.