Data Processing Addendum

This Data Processing Addendum ("DPA") forms a part of the Agreement between Airia and Customer. This DPA is incorporated into the Agreement by reference and describes the Parties' obligations regarding the Processing of Personal Information. Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name of and on behalf of its Authorized Affiliates, if and to the extent that Airia Processes Personal Information for such Authorized Affiliates that qualify as a Controller. Airia is acting as a Service Provider and Processor. All capitalized terms not defined shall have the meanings provided in the Agreement. In the event of a conflict between the terms of the Agreement and the DPA, this DPA shall prevail.

1. ***Definitions***.

"Affiliates" means any legal entity controlling, controlled by or under common control with a party to this DPA, for so long as such Control relationship exists.

"Authorized Affiliates" means those certain Customer Affiliates that, if agreed upon by Airia, are authorized to utilize the Airia Services as Users pursuant to the Agreement.

"Applicable Data Protection Law(s)" means any applicable law, ordinance, statute, regulation, or other binding restriction to which the Personal Information is subject, including but not limited to CCPA, GDPR, UK GDPR, Data Protection Act 2018 and Non-EU Data Protection Laws, and all amendments thereof.

"Control" means the ownership of more than 50% of the applicable entity or the ability in fact to direct the management decisions of such entity.

"Customer Personal Information" means Personal Information belonging to Customer that is processed by Airia in the course of providing the Airia Services under the Agreement.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Information.

"Data Subject" has the meaning assigned to the term "data subject" or "consumer" under Applicable Data Protection Laws and shall include identified or identifiable natural persons to whom the Personal Information relates.

"GDPR" means the EU General Data Protection Regulation 2016/679.

"Non-EU Data Protection Laws" means US state comprehensive privacy laws, including but not limited to the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), and any implementing regulations or guidance provided by the California Attorney General ("CCPA") and Canada's Personal Information Protection and Electronic Documents Act, S.C., 2000, ch. 5 ("PIPEDA") and any provincial legislation deemed substantially similar to PIPEDA pursuant to the procedures set forth within PIPEDA, and all amendments to the CCPA, PIPEDA and similar legislation, as they may be enacted, from time to time.

"Personal Information" means any data provided by Customer or its Authorized Affiliates to Airia that identifies or, alone or in combination with any other data, could reasonably be used to identify, locate, or contact a natural person or household, or any other information that is considered "personally identifiable information," "personal information," "personal data," or other similar terms under Applicable Data Protection Laws, but does not include data or information that is publicly available within the meaning of such section or that has been de-identified within the meaning of Applicable Data Protection Laws.

"Process" or "Processing" means any operation or set of operations that are performed upon Personal Information, whether or not by automatic means, such as collection, accessing, processing, use, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, transmittal, alignment or combination, blocking, erasure, destruction or otherwise used as set out in the Applicable Data Protection Laws.

"Security Incident" means any situation in which Airia confirms that Personal Information under its direct control has been accessed, acquired, disclosed, altered, lost, destroyed, or used by unauthorized persons in an unauthorized manner having a material impact on Customer or its Affiliates or on Data Subject rights.

"Sell," "selling," "sale," or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's

Personal Information to a third party for monetary or other valuable consideration.

"Share", "sharing", or "shared" means the provision of Personal Information to support targeted advertising across unaffiliated websites based on online behavioral profiling.

"Service Provider" means an entity that processes information on behalf of Customer and to which Customer discloses a Data Subject's Personal Information for a business purpose pursuant to a written contract.

"Sub-Processor(s)" means any third-party service provider of Airia and to whom Airia provides or makes available Personal Information for Processing to be carried out on behalf of Customer or its Authorized Affiliates. For clarity, Sub-processors do not include Third-Party Services with whom Customer or its Authorized Affiliates directs Airia to interact with or disclose Personal Information. Airia may disclose Personal Information to such Third-Party Services, and Airia shall have no responsibility for the use of any Personal Information by any such third parties.

2. ***Service Provider Relationship; Restrictions and Use of Personal Information.*** Customer appoints Airia as a Service Provider of Personal Information and is disclosing Personal Information to Airia in that capacity exclusively for the execution of Airia Services detailed in the Agreement. Customer and its Authorized Affiliates agree that Airia may use Personal Information for purposes of performing its obligations under the Agreement and as otherwise contemplated in the Agreement. Airia agrees: (i) each Airia employee handling Personal Information will be subject to a duty of confidentiality; (ii) it will promptly notify Customer upon determining Airia can no longer meet its obligations under relevant Applicable Data Protection Laws or this DPA; (iii) it will not retain, use, or disclose Personal Information for any purpose not permitted by the Agreement or Applicable Data Protection Laws; (iv) it will not Sell or Share Personal Information; (v) it will not combine or update Personal Information received in connection with performing Airia Services under the Agreement and this DPA with Personal Information Airia receives from another source; and (vi) it will not attempt to or actually re-identify any aggregated, de-identified, or anonymized Customer Data.

3. ***Customer Obligations***. Customer and its Authorized Affiliates warrant that they: (i) will comply with obligations under Applicable Data Protection Laws, including applicable obligations as a Data Controller; (ii) have provided all notices and obtained all consents and rights necessary under Applicable Data Protection Laws for Airia to Process Personal Information and provide the Airia Services; (iii) will ensure that there is at all times a sufficient legal basis for Airia's Processing as permitted under this DPA; and (iv) will limit the provisioning of Personal Information to Airia only to the amount and kinds of data adequate, relevant, and necessary for performing the Airia Services. Without limiting any payment obligations under the Agreement, Customer shall immediately notify Airia and cease use of the Airia Services in the event any required authorization or legal basis for Processing is revoked or terminated, or, for notification purposes only, promptly notify Airia if it discovers any unauthorized access to its Environment or Customer Data.

4. ***Privacy Inquiries and Requests***. Customer is responsible for handling any Privacy Inquiry and Privacy Request (as defined below) from Data Subjects with respect to their Personal Information Processed by Airia. Airia agrees to assist Customer and provide Customer the information and assistance required under Applicable Data Protection Laws to enable Customer to respond to: (i) questions or complaints received from Data Subjects regarding Personal Information ("Privacy Inquiry"); and (ii) requests from Data Subjects exercising their rights in Personal Information granted to them under Applicable Data Protection Laws ("Privacy Request"). Airia will respond within a reasonable time which permits Customer to respond to the Privacy Inquiry or Privacy Request in accordance with the timelines set forth in Applicable Data Protection Laws. If Airia is directly contacted with a Privacy Inquiry or Privacy Request, Airia will promptly forward such inquiry to Customer. Customer shall inform Airia of any Data Subject request made pursuant to Applicable Data Protection Laws with which Airia is required to comply and will provide all reasonable information necessary for Airia to comply with the request. Privacy-related requests may be submitted to privacy@airia.com.

5. ***Data Protection Impact Assessment***. Taking into account the Airia Services provided and the information available to Airia, Airia shall cooperate with Customer, at Customer's expense, to enable Customer to conduct data protection impact assessment(s) required for Customer to comply with Applicable Data Protection Laws.

6. ***Security***. Airia has implemented and shall maintain reasonable and appropriate technical and organizational measures designed to protect Personal Information from a Security Incident and to protect the rights of the relevant Data Subjects as defined in Applicable Data Protection Laws. Such security measures are further detailed in the attached Annex II.

7. ***Security Incident***. Upon becoming aware of a Security Incident, Airia will inform Customer without undue delay and provide timely information to enable Customer to timely fulfill its reporting obligations required under

Applicable Data Protection Laws. If the Security Incident was caused by Airia, Airia shall further take reasonable measures to remedy or mitigate the effects of the Security Incident and will keep Customer reasonably informed of such measures.

8. ***Audits***. Upon Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Airia shall make available to Customer or, subject to Airia's approval, Customer's independent, third-party auditor (provided Customer remains responsible for an approved auditor's compliance with the confidentiality obligations in the Agreement) information regarding Airia's compliance with the obligations set forth in this DPA in the form of, at Airia's option, (i) answering a security questionnaire, or, as available, (ii) providing third-party certifications and audits. Airia shall respond within a reasonable timeframe to Customer requests for documentation that verifies that it no longer retains or uses Personal Information that has been subject to a valid deletion request to Customer.

9. ***Deletion or Return of Data***. Upon termination or expiry of the Agreement, Airia may delete Customer Data pursuant to the Agreement, or, subject to Customer paying applicable fees, return Customer Data to Customer, unless retention is required by law. Customer acknowledges that Airia is not a system of record and, accordingly, Customer will maintain its own copies of its essential business records.

10. ***Sub-processor(s)***. Customer hereby provides general authorization to Airia to engage third party Sub-processors to Process any Personal Information, with the current list of Sub-processors shown here ("Sub-Processor Table"). Airia will impose data protection terms on any Sub-processor it appoints designed to protect the Personal Information with substantially the same standard provided for by this DPA. Airia may make changes to its Sub-Processors in its sole discretion, provided: (i) it shall inform Customer of any intended changes concerning its Sub-Processors by updating the Sub-Processor Table; and (ii) Customer may object in writing to Airia's appointment of a new Sub-Processor within thirty (30) days of such appointment so long as the objection is based on reasonable data privacy or security concerns. Airia will not use a new Sub-Processor until such thirty (30) days have passed (except in the event of an emergency). If Customer submits an objection to a new Sub-Processor, the Parties will work together to find an agreed upon solution. If no solution is agreed upon within the thirty (30) day period, Customer may terminate the Agreement.

11. ***International Transfers***. If Airia Processes, accesses, or stores Personal Information in a third country (as defined in the GDPR and UK GDPR), then the Parties agree that, and only to the extent applicable, Airia's Data Privacy Framework EU-US and UK Extension compliance ("DPF Compliance") shall apply. If DPF Compliance is not applicable,the Standard Contractual Clauses for the transfer of Personal Information to data processors established in third countries set out in the Commission Decision of 5 February 2010 (C(2010) 593), as amended by EU Commission Implementing Decision 2021/914 of 4 June 2021, and as may be further amended from time to time ("SCCs") found here shall be deemed agreed and incorporated herein by reference, and if applicable, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force March 21, 2022 ("UK Addendum"), currently found here applies to the relevant exports from the United Kingdom (with Tables 1-3 being interpreted in accordance with the SCCs Controller to Processor (Module 2); Table 2 being the "version of the Approved EU SCCs which this Addendum is appended to" option is selected; and Table 4 having the Importer and Exporter selected) shall also apply. If one or both of the foregoing are not applicable or Applicable Data Protection Laws require a different approach, the Parties agree that they will work together in good faith to ensure the protection of the Personal Information being transferred meet applicable requirements. To the extent that Airia and Customer are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently revoked or held in a court of competent jurisdiction to be invalid, Airia will, in good faith, pursue a suitable alternate mechanism that can lawfully support the transfer.

12. ***Data Localization Restrictions***. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer shall not use or access the Airia Services in a manner that would require Customer Data, Personal Information, or its Environment to be hosted in or localized to a specific country pursuant to such country's Applicable Data Protection Laws.

13. **Artificial Intelligence Governance.** The Parties acknowledge laws and regulations relating to artificial intelligence use and provisioning are often being proposed, implemented, and changed ("AI Regulations"). If AI Regulations cause this DPA to be invalid, the Parties agree to work together in good faith to amend this DPA so that it is compliant with AI Regulations. If AI Regulations cause Airia to be unable to provide the Airia Services, either Party may terminate the Agreement provided such a termination will not relieve either Party's obligations and liabilities incurred up to the date of the termination.

14. ***Miscellaneous***. Customer may request Airia to accept additional data privacy terms necessary to address

Applicable Data Protection Laws. If Airia does not agree to such additional data privacy terms, Airia may terminate the DPA without penalty on thirty (30) days' written notice. Except as amended by this DPA, all terms and conditions of the Agreement shall remain in full force and effect. Nothing in this DPA or the Agreement relieves Customer of its own direct responsibilities and liabilities under Applicable Data Protection Laws.

Annex I: Description of Transfers

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Information into the Airia Service, the extent of which is determined and controlled solely by the data exporter, and which may include, but is not limited to Personal Information relating to the following categories of data subjects:

Data exporter's employees, contractors, representatives, agents, and other individuals whom data exporter allows and is permitted to use the Airia Service, as well as Personal Information relating to the data exporter's customers, partners, users, vendors, and other categories as otherwise contemplated by the Agreement.

Categories of personal data transferred

Data exporter may submit Personal Information to the Airia Services, the extent of which is determined and controlled solely by data exporter, and which may include, but is not limited to the following Personal Information:

First and last name, contact information such as address, telephone number, and email address, IP address, user identifier, and other categories as otherwise contemplated by the Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Any special categories of personal data or sensitive Personal Information, in the sole discretion of Data exporter, which may be included in an Input or otherwise Customer Data submitted into the Airia Services or contained in an Output generated by the Airia Services. Notwithstanding the foregoing, Customer may not submit any Protected Health Information (as defined in the Health Insurance Portability and Accountability Act of 1996) unless the Airia BAA is entered into by the Parties. No PCI-DSS-related data (except to enter in its payment information for the Airia Services), biometric data, or other sensitive data types shall be submitted to Airia or into the Airia Services. If Customer ignores the foregoing restrictions, Customer is fully responsible for such data and Airia disclaims all liability relating to any claims involving such data.

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

Continuous basis until termination or expiration of the Agreement.

Nature of the processing

The performance of the Airia Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The performance of the Airia Services pursuant to 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 until it is deleted in accordance with the Agreement.

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

As stated above, and as may be further detailed in the Sub-Processor Table made available and updated by Airia from time to time.

ANNEX II: Security Measures

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) 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.

Airia's information security program, as established through its Information Security Policy's internal controls and procedures, is designed to ensure: (i) Customer Data Airia processes is protected against accidental, unlawful, or unauthorized loss, access, or disclosure; (ii) reasonably foreseeable risks relating to security and unauthorized access are identified and protected against; and (iii) security risks are minimized by implementing, maintaining, and regularly assessing such controls.

Access Controls

Airia has instituted access control management policies: (i) governing the security of Airia's information, networks, applications, and systems aimed to prevent unauthorized access to such items; and (ii) relating to Airia's networks, applications, and systems to ensure only authorized users access appropriate information based on their role and to prevent unauthorized access to the same.

Encryption and Key Management

All encryptions for data and relating to key management shall be end-to-end and be performed in accordance with industry standards, including NIST SP 800-57. The below represents Airia's encryption methods for at-rest and in-transit data.

- At-Rest: AES 256 bit symmetric encryption
- In-Transit: TLS 1.2 (minimum)

Asset Management

Airia has instituted policies that appropriately identify and classify its assets to ensure their security and integrity. Protection levels are established pursuant to the corresponding asset's importance and exposure to sensitive information, and are designed to prohibit unauthorized disclosures, loss, damage, or destruction of information in relation to the asset.

Contingency Planning

Airia has instituted redundancy controls to eliminate single points of failure and minimize the impact of possible physical and environmental risks. It has also established a Business Continuity and Disaster Recovery Plan, which it tests regularly, to help ensure the Airia Services' continuity.

Security Incident Response

Airia has instituted policies to minimize a security incident's impact, including as it relates to the availability and confidentiality of the Airia Services. These policies help Airia to efficiently respond, mitigate, handle, and communicate issues relating to a security incident.

Risk Management

- Internal – Institute policies relating to managing potentials risks, including conducting risk assessments and corresponding mitigation efforts regarding loss, unavailability, damage, or unauthorized access to Airia's information, networks, or controls.
- External (Including System Governance) - Airia has instituted policies and controls for Airia to vet its vendors to establish appropriate security measures, including contract reviews to ensure appropriate controls and systems are in place and conducting due diligence to effectively on-board and off-board Airia vendors. Once a vendor is on-boarded, Airia has instituted policies relating to the monitoring, developing, and supporting of the on-boarded systems and solutions.

Security Controls

- Network – institute policies to protect Airia's network generally, including protecting the transferring of information, network security, segregated networks, and network services as information is processed and transferred.

- Operational – institute policies ensuring the secure management of its information technology systems relating to system integrity, protecting against the exploitation of technical vulnerabilities, malware, and data loss, and standardizing backups, logging, installations, and change management.
- Physical – institute policies relating to physical and environmental threats by identifying security and access controls regarding personnel, visitors, equipment, secure/controlled areas, threat detection, destruction of data, and office documentation and organization management to prohibit unauthorized access and the loss or damage to Airia's systems, data, and operations.
- Personnel – institute policies relating to hiring standards and procedures, including appropriate vetting of prospective personnel, background check requirements, and utilizing appropriate confidentiality and employment-related agreements. The policies also institute on-going security and data privacy training for personnel to protect Airia's systems, networks, and controls during the entire employment lifecycle.