Last Updated: October 2nd, 2026

Data Processing Addendum

This Data Processing Addendum ("**DPA**") is 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 Affiliates (if and to the extent that Airia Processes Personal Information for such Affiliates that qualify as a Controller). Airia is acting as a Processor and (where applicable) a Sub-Processor. All capitalized terms not defined in **Section 21** or another Section of this DPA shall have the meanings provided in the Agreement.

1. **Appointment.** Customer appoints Airia as a Processor (or Sub-Processor, as applicable) of Personal Information and is disclosing Personal Information to Airia in that capacity exclusively for the provision of Airia Services detailed in the Agreement. Customer and its 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: (a) each Airia employee handling Personal Information will be subject to a duty of confidentiality; (b) it will promptly notify Customer upon determining Airia can no longer meet its obligations under relevant Applicable Data Protection Laws or this DPA; (c) it will not retain, use, or disclose Personal Information for any purpose not permitted by the Agreement or Applicable Data Protection Laws; and (d) it will not combine or commingle Customer's Personal Information with the personal information of any other Airia customer. If the CCPA governs Customer's use of the Airia Services, then Customer shall also appoint Airia as a Service Provider (as defined in the CCPA) and **Annex IV: CCPA Terms** shall also apply.

2. **Documented Instructions.** Airia and its Sub-Processors will Process Personal Information only in accordance with the documented instructions of Customer. The Agreement, including this DPA, constitutes Customer's primary documented instructions to Airia regarding the Processing of Personal Information, including for purposes of the applicable international transfer mechanism pursuant to Sections 11 to 14 of this DPA. Airia will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and Applicable Data Protection Law.

3. **Customer Obligations**. Customer and its Affiliates warrant that they: (a) will comply with Applicable Data Protection Laws, including applicable obligations as a Controller and (where applicable) a Processor; (b) 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; (c) will ensure that there is at all times a sufficient legal basis for Airia's Processing as permitted under this DPA; and (d) will limit the provisioning of Personal Information to Airia only to the amount and types of data adequate, relevant, and necessary for performing the Airia Services. Without limiting any payment obligations under the Agreement, Customer shall promptly notify Airia and cease use of the Airia Services in the event any required authorization or legal basis for Processing is revoked or terminated and promptly notify Airia if it discovers any unauthorized access to its Personal Information. Nothing in this DPA relieves Customer of its own direct responsibilities and liabilities under Applicable Data Protection Laws.

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 provide Customer the information and assistance required under Applicable Data Protection Laws to enable Customer to respond to: (a) questions or complaints received from Data Subjects regarding Personal Information ("**Privacy Inquiry**"); and (b) requests from Data Subjects exercising their rights in Personal Information granted to them under Applicable Data Protection Laws ("**Privacy Request**"). Airia will respond no later than 7 days after receiving a Privacy Inquiry or Privacy Request (or such shorter period as is necessary to enable Customer to meet any applicable statutory deadline), providing information sufficient to enable Customer to respond 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. Customer shall submit privacy-related requests to privacy@airia.com.

5. **Data Protection Impact Assessment**. Upon Customer's request, Airia shall provide Customer with such reasonable cooperation and assistance as is needed to fulfill Customer's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Airia Services (to the extent Customer does not otherwise have access to the relevant information and such information is available to Airia).

6. **Security**. Airia has implemented and shall maintain technical and organizational measures which are appropriate to the

Copyright © Airia LLC 2026

risk and which are designed to protect Personal Information from a Security Incident, to preserve the confidentiality, integrity, and availability of Personal Information, and to protect the rights of the relevant Data Subjects as defined in Applicable Data Protection Laws. Such security measures are further detailed in **Annex II: Security Measures**. If the Customer's access to the Airia Services includes any security controls, features, and functionalities (as further detailed in the Documentation), Customer is responsible for implementing those measures to enhance the security of the Personal Information.

7. **Security Incident**. Upon becoming aware of a Security Incident, Airia will inform Customer without undue delay and provide information required by Applicable Data Protection Laws to enable Customer to fulfill its reporting obligations required under Applicable Data Protection Laws. Where complete information is not yet available, Airia will provide an initial notification followed by updates as further details become known. 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 (not to be unreasonably withheld or delayed), Customer's independent, third-party auditor (provided Customer remains responsible for an approved auditor's compliance with the confidentiality obligations in the Agreement) copies of, or extracts from, Airia's audit reports related to the security of the Airia Services, including, for example, its ISO 27001 certification and/or SOC 2 Type 2 report in order to verify Airia's compliance with the obligations set forth in this DPA ("**Information Request**"). Airia shall also 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 lawful deletion request by Customer (including a request Customer submits on behalf of a Data Subject). Where Airia's compliance with this DPA cannot be verified through an Information Request, Customer may request an audit ("**Audit**"). An Audit must meet the following requirements: (a) Customer must provide Airia at least 60 days' prior written notice of a proposed Audit unless otherwise required by a competent supervisory authority or Applicable Data Protection Laws; (b) Customer may not perform more than one Audit in any 12-month period, except where required by a competent supervisory authority; (c) Customer and Airia must mutually agree on the time, scope, and duration of the Audit in advance; (d) Customer must reimburse Airia for its time expended in connection with an Audit at Airia's reasonable professional service rates, which will be made available to Customer on request; (e) Customer must ensure that its representatives performing an Audit protect the confidentiality of all information obtained through the Audit in accordance with the Agreement; and (f) remote Audits shall be utilized where possible, with on-site Audits occurring only where a walkthrough of the premises is required.

9. **Deletion or Return of Data.** Following termination of the Agreement, Customer shall (if it notifies Airia in writing of its request) have 30 days to export its Personal Information from the Airia Services and after such time has passed Airia shall destroy all Personal Information in its possession or control and, upon Customer's written request, provide a written certification of such destruction. This requirement shall not apply to the extent that: (a) Airia is required by applicable law to retain some or all of the Personal Information; or (b) Personal Information is archived on Airia's back-up and support systems, which shall be deleted in accordance with its security procedures, provided that Airia shall continue to protect such Personal Information in accordance with its obligations herein.

10. **Sub-Processors.** 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 at https://trust.airia.com/subprocessors ("**Sub-Processor Table**"). Airia will impose data protection terms on any Sub-Processor it appoints which are designed to protect the Personal Information with substantially the same standard provided for by this DPA. Airia may make changes to its Sub-Processors, provided: (a) it shall inform Customer of any intended changes concerning its Sub-Processors by updating the Sub-Processor Table; and (b) Customer may object in writing to Airia's appointment of a new Sub-Processor within 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 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 30-day period, Customer may terminate the Agreement.

11. **Data Privacy Framework**. Customer acknowledges that Airia complies with the Data Privacy Framework and that transfers of Personal Information to Airia made under the Data Privacy Framework shall not be a Restricted Transfer. Airia will notify Customer if its Data Privacy Framework certification lapses or is otherwise invalidated, in which event any transfers of Personal Information from Customer to Airia shall be deemed a Restricted Transfer and the provisions of **Annex III**: **Standard Contractual Clauses** shall apply without the Parties being required to take any further action.

12. **Restricted Transfers**. Before undertaking any Restricted Transfer, Airia shall review the adequacy of data protection in the Third Country and shall apply (where necessary) the appropriate measures to ensure that the Personal Information transferred is subject to an essentially equivalent protection as that guaranteed in its original jurisdiction. If at any time Airia is unable to comply with its legal or contractual obligations related to international transfers under European Data

Copyright © Airia LLC 2026

Protection Laws it shall notify Customer and suspend the applicable transfers of Personal Information until it is able to comply with such obligations.

13. **Restricted Transfers to Airia**. In connection with the Airia Services, the Parties anticipate that Airia (and its Sub-Processors) may Process Personal Information outside of the EEA, Switzerland, and the UK that is protected by European Data Protection Laws in respect of which Customer or its Affiliates may be a Controller (or Processor on behalf of a third-party Controller, as applicable). The Parties agree that when the transfer of Personal Information protected by European Data Protection Laws from Customer or its Affiliates to Airia is a Restricted Transfer, then the provisions of **Annex III**: **Standard Contractual Clauses** shall apply. If the Data Privacy Framework is subsequently revoked or held by a court of competent jurisdiction to be invalid, then the provisions of **Annex III**: **Standard Contractual Clauses** shall apply without the Parties being required to take any further action. Additionally, to the extent that Airia and Customer are relying on any other specific statutory mechanism to comply with Applicable Data Protection Laws and that mechanism is subsequently revoked or held by a court of competent jurisdiction to be invalid, Airia will, in good faith pursue a suitable alternate mechanism that can lawfully support the transfer.

14. **Restricted Transfers to Sub-Processors**. With respect to Restricted Transfers made to Airia, Airia may neither participate in, nor permit any Sub-Processor to participate in, any further Restricted Transfer unless the further Restricted Transfer is made in compliance with Applicable Data Protection Laws and a legally compliant transfer mechanism.

15. **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 Content, Personal Information, or its environment to be hosted in or localized to a specific country pursuant to such country's Applicable Data Protection Laws.

16. **Government Access Requests.** If Airia receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Customer's Personal Information, Airia will, to the extent legally permitted, attempt to: (a) redirect the governmental body to request such Personal Information directly from Customer; and (b) challenge any demand that appears overbroad, procedurally defective, or otherwise not in compliance with applicable law through appropriate legal process. As part of this attempt, Airia may provide Customer's basic contact information to the governmental body. If compelled to disclose the Personal Information to a governmental body, Airia will give Customer reasonable advance notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Airia is legally prohibited from doing so. In any event, Airia will disclose only the minimum amount of Personal Information strictly necessary to satisfy the legal demand.

17. **Affiliates.** Airia's obligations in this DPA shall also extend to Customer's Affiliates, subject to the following conditions: (a) Customer is solely responsible for communicating any additional processing instructions on behalf of its Affiliates; (b) Customer shall be responsible for its Affiliates' compliance with this DPA and all acts and/or omissions by an Affiliate with respect to Customer's obligations under this DPA; and (c) if an Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Airia ("**Affiliate Claim**"), Customer must bring such Affiliate Claim directly against Airia on behalf of such Affiliate, unless Applicable Data Protection Laws require the Affiliate be a party to such claim, and all Affiliate Claims shall be considered claims made by Customer. In no event will this DPA or any Party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

18. **Change in Law**. If any change in Applicable Data Protection Laws (a "**Change in Law**") materially affects either Party's ability to perform its obligations under this DPA or renders any provision of this DPA non-compliant, inadequate, or unenforceable, the Parties shall negotiate in good faith such amendments to this DPA as are reasonably necessary to address the Change in Law and ensure continued compliance. Either Party may initiate such negotiations by providing written notice to the other Party describing the Change in Law and the proposed amendments. The Parties shall use commercially reasonable efforts to agree upon and execute such amendments within a reasonable time, and in any event prior to the effective date of the Change in Law where practicable.

19. **Aggregate Liability**. Notwithstanding anything to the contrary in the Agreement and to the maximum extent permitted by law, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, the SCCs or any data protection agreements in connection with the Agreement (if any), whether in contract, tort or under any other theory of liability, shall remain subject to Section 7 (Liability) of the Terms.

20. **Law & Jurisdiction.** This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

21. **Definitions**.

"**Adequate Country**" a country that the European Commission, the United Kingdom's Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner (as applicable based on respective area of competence) has determined as ensuring an adequate level of data protection.

Copyright © Airia LLC 2026

"**Applicable Data Protection Law(s)**" any applicable law, ordinance, statute, regulation, or other binding restriction to which the Personal Information is subject, including but not limited to European Data Protection Laws and US Data Protection Laws, and all amendments thereof.

"**Controller**" 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 Privacy Framework**" the EU-U.S. Data Privacy Framework, the UK-U.S. extension to the EU-U.S. Data Privacy Framework and the Swiss-US Data Privacy Framework as set forth by the U.S. Department of Commerce.

"**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.

"**European Data Protection Laws**" all laws and regulations of the European Union ("**EU**"), the European Economic Area ("**EEA**"), their member states, Switzerland, and the United Kingdom ("**UK**") applicable to the processing of Personal Information under the Agreement (including, where applicable, (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (b) the EU GDPR as saved into UK law by virtue of section 3 of the UK's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "**UK GDPR**"); (c) the Swiss Federal Act on Data Protection of 25 September 2020 and its corresponding ordinances ("**Swiss FADP**"); (d) the EU e-Privacy Directive (Directive 2002/58/EC); and (e) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (a), (b), (c) and (d)).

"**EU SCCs**" the standard contractual clauses for international transfers annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

"**Personal Information**" any data provided by Customer or its 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 "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 Applicable Data Protection Laws or that has been de-identified within the meaning of Applicable Data Protection Laws.

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

"**Processor**" the entity that Processes Personal Information on behalf of a Controller.

"**Restricted Transfer**" (a) where the EU GDPR or Swiss FADP applies, a transfer of Personal Information from the EEA or Switzerland (as applicable) to a country outside of the EEA or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); or (b) where the UK GDPR applies, a transfer of Personal Information from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018. For the avoidance of doubt, a transfer of Personal Information to the United States pursuant to the Data Privacy Framework shall not be a Restricted Transfer.

"**SCCs**" the EU SCCs and the UK Transfer Addendum.

"**Security Incident**" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed for the purpose of providing the Airia Services to Customer.

"**Sub-Processor(s)**" any third-party service provider of Airia to whom Airia provides or makes available Personal Information for Processing to be carried out on behalf of Customer or its Affiliates.

"**Third Country**" a country outside of the EEA, the UK or Switzerland (as applicable) which is not an Adequate Country.

"**UK Transfer Addendum**" the International Data Transfer Addendum (Version B1.0) issued by the Information Commissioner's Office under section 119A of the Data Protection Act 2018, as updated or amended from time to time.

"**US Data Protection Laws**" US state comprehensive privacy laws, including but not limited to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (Cal. Civ. Code §§ 1798.100–1798.199) ("**CCPA**").

Copyright © Airia LLC 2026

Annex I: Description of Transfers

List of Parties

Data exporter(s)**:**

Name: Customer and any Affiliates.	As stated in the Agreement
Address: Addresses of Customer and any Affiliates described in the Agreement (or otherwise notified by Customer to Airia)	As stated in the Agreement
Contact person's name, position and contact details:	As stated in the Agreement
Activities relevant to the data transferred under this DPA and the SCCs:	Use of the Airia Services pursuant to the Agreement
Signature and date:	This Annex I shall be deemed executed upon execution of the Agreement incorporating this DPA
Role (controller/processor):	Controller (or Processor on behalf of a third-party Controller)

Data importer(s):

Name:	Airia LLC
Address:	PO Box 190778, Miami Beach, FL 33119
Contact person's name, position and contact details:	John DiRico Data Protection Officer privacy@airia.com
Activities relevant to the data transferred under this DPA and the SCCs:	Processing necessary to provide the Airia Services to Customer, pursuant to the Agreement.
Signature and date:	This Annex I shall be deemed executed upon execution of the Agreement incorporating this DPA.
Role (controller/processor):	Processor (or Sub-Processor)

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Information into the Airia Services, 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 Services, 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:

Copyright © Airia LLC 2026

Account data of Users: names, job titles and contact information such as address, telephone number and email address. Authentication credentials of Users.

Usage data: IP addresses, session and user ID, user-related metadata (timestamps).

To the extent any of the following contain Personal Information:

Content: communications with Models (messages from Users, document uploads and AI-generated responses) and any other Content submitted to Airia or the Airia Services in the course of Airia providing the Airia Services.

Configuration data: stored prompts, assistants, workflows and knowledge bases.

Integration: data from Third-Party Services and Customer Applications configured to operate with the Airia Services.

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.

Data exporter may submit special categories of Personal Information or sensitive Personal Information to the Airia Services, the extent of which is determined and controlled solely by data exporter. Notwithstanding the foregoing, Customer may not submit any protected health information (as defined in the Health Insurance Portability and Accountability Act of 1996) unless a Business Associate Agreement is entered into by the Parties. No PCI-DSS-related data (except to enter 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.

Copyright © Airia LLC 2026

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: (a) Content Airia processes is protected against accidental, unlawful, or unauthorized loss, access, or disclosure; (b) reasonably foreseeable risks relating to security and unauthorized access are identified and protected against; and (c) security risks are minimized by implementing, maintaining, and regularly assessing such controls.

Access Controls

Airia has instituted access control management policies: (a) governing the security of Airia's information, networks, applications, and systems aimed to prevent unauthorized access to such items; and (b) 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 – implements and maintains policies to manage potential 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.

Copyright © Airia LLC 2026

Security Controls

- Network – implements and maintains controls protecting Airia's network generally, including protecting the transferring of information, network security, segregated networks, and network services as information is processed and transferred.
- Operational – implements and maintains controls 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 – implements and maintains controls addressing 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 – implements and maintains controls governing 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 ongoing security and data privacy training for personnel to protect Airia's systems, networks, and controls during the entire employment lifecycle.

Copyright © Airia LLC 2026

Annex III: Standard Contractual Clauses

1. **Transfers from the EEA**. Where a Restricted Transfer is made of Personal Information protected by the EU GDPR, the EU SCCs are incorporated into this DPA and apply to the transfer as follows:

   a) Module Two applies where Customer is a Controller and Airia is a Processor, and Module Three applies where both Customer and Airia are Processors;
   b) in Clause 7, the optional docking clause does not apply;
   c) in Clause 9(a) of Modules Two and Three, Option 2 applies, and the period for prior notice of Sub-Processor changes is set forth in **Section 10 (Sub-Processors)** of this DPA;
   d) in Clause 11(a), the optional language does not apply;
   e) in Clause 13, the competent supervisory authority is the Irish Data Protection Commission;
   f) in Clause 17, Option 1 applies with the governing law being that of the Republic of Ireland;
   g) in Clause 18(b), disputes will be resolved before the courts in Dublin, Republic of Ireland;
   h) Annex I of the EU SCCs is completed with the information in **Annex I: Description of Transfers** to this DPA;
   i) Annex II of the EU SCCs is completed with the information in **Annex II**: **Security Measures** to this DPA;
   j) Annex III of the EU SCCs is completed with the information in the Sub-Processor Table; and
   k) the Parties agree that Airia's liability to Customer under Clause 12 shall be subject to the liability limitations and exclusions contained in the Agreement and/or this DPA.

2. **Transfers from the UK.** Where a Restricted Transfer is made of Personal Information protected by the UK GDPR, the EU SCCs as completed in accordance with **Section 1 (Transfers from the EEA)** are incorporated into this DPA and shall apply to the transfer, except that:

   a) the EU SCCs shall be deemed amended as specified by the UK Transfer Addendum;
   b) any conflict between the terms of the EU SCCs and the UK Transfer Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Transfer Addendum;
   c) Table 2 is completed by reference to **Section 1 (Transfers from the EEA**) and Tables 1 and 3 shall be deemed completed using the information contained in **Annex I: Description of Transfers** and **Annex II**: **Security Measures**; and
   d) Table 4 in Part 1 of the UK Transfer Addendum shall be deemed completed by selecting "neither party."

3. **Transfers from Switzerland**. Where a Restricted Transfer is made of Personal Information protected by the Swiss FADP, the EU SCCs as completed in accordance with **Section 1 (Transfers from the EEA)** are incorporated into this DPA and shall apply to the transfer, except that:

   a) in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner;
   b) references to "Member State" in the EU SCCs refer to Switzerland, and data subjects located in Switzerland may exercise and enforce their rights under the EU SCCs in Switzerland; and
   c) references to the "General Data Protection Regulation," "Regulation 2016/679," and "GDPR" in the SCCs refer to the Swiss Federal Act on Data Protection (as amended or replaced).

4. **Specific application of the SCCs.** The following terms apply to the SCCs**:**

   a) Customer may exercise its audit rights under the SCCs as set out in **Section 8 (Audits)** of this DPA;
   b) Airia may appoint Sub-Processors under the SCCs as set out in **Section 10 (Sub-Processors)** of this DPA; and
   c) If any provision of this **Annex III: Standard Contractual Clauses** is inconsistent with any terms in the SCCs, the SCCs prevail.

Copyright © Airia LLC 2026

Annex IV: CCPA Terms

1. **Definitions.**

For the purpose of these CCPA Terms, the terms "**Commercial Purpose**", "**Consumer**", "**Personal Information**", "**Sell**", "**Service Provider**", and "**Share**" have the meanings given to them in the CCPA.

2. **Airia Obligations.**

Airia will (a) not Sell or Share Personal Information; (b) process Personal Information only to provide, support, and improve the Airia Services in accordance with the Agreement, or as otherwise permitted under the CCPA; (c) not retain, use, or disclose Personal Information (i) for any purpose, including any Commercial Purpose, except to provide, support, and improve the Airia Services in accordance with the Agreement, or as otherwise permitted under the CCPA, (ii) outside the direct business relationship between Airia and Customer, or (iii) in any way prohibited by the CCPA; (d) not combine the Personal Information it receives from, or on behalf of, Customer with Personal Information it receives from, or on behalf of, another person or from Airia's own interactions with the Consumer to whom the Personal Information relates, except to the extent a Service Provider is permitted to do so under the CCPA; (e) comply with all applicable obligations under, and provide the same level of privacy protection to Personal Information as required by, the CCPA; (f) notify Customer if it believes it cannot meet its obligations under the CCPA; and (g) on Customer's request and taking into account the nature of the Personal Information processed, provide reasonable assistance to Customer in fulfilling Consumer requests made under the CCPA to the extent Customer is unable through its use of the Airia Services to address a particular request on its own.

3. **Customer's Obligations and Rights.**

Customer may (a) only disclose Personal Information to Airia for the limited purpose of using the Airia Services in accordance with the Agreement; and (b) upon notice to Airia, take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Airia.

Copyright © Airia LLC 2026