Last Updated: October 2nd, 2026

Standard Contractual Clauses Amendment

This Standard Contractual Clauses Amendment ("**SCC Amendment**") is entered into by and between Airia LLC ("**Airia**") and the customer signing this SCC Amendment ("**Customer**" and together with Airia, the "**Parties**").

This SCC Amendment supplements and forms part of the Data Processing Addendum between the Parties ("**DPA**"), which is itself incorporated into the agreement governing Customer's use of the Airia Services ("**Agreement**"). In the event of any conflict between this SCC Amendment and the DPA or Agreement, this SCC Amendment shall prevail to the extent of the conflict as it relates to Restricted Transfers (defined below).

This SCC Amendment shall terminate and replace any prior versions of the standard contractual clauses which are part of the Agreement immediately prior to this SCC Amendment becoming effective.

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

1. **Purpose.** This SCC Amendment sets out the terms pursuant to which the Parties comply with applicable requirements for the international transfer of Personal Information protected by European Data Protection Laws, by incorporating and configuring the applicable SCCs into the DPA.

2. **Transfers from the EEA**. Where a Restricted Transfer is made of Personal Information protected by the EU GDPR, the EU SCCs are incorporated into the 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 the 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** below;
    i) Annex II of the EU SCCs is completed with the information in **Annex II**: **Security Measures** below;
    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 the DPA.

3. **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 2 (Transfers from the EEA)** are incorporated into the 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 2 (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."

4. **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 2 (Transfers from the EEA)** are incorporated into the 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).

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

Copyright © Airia LLC 2026

a) Customer may exercise its audit rights under the SCCs as set out in Section 8 (Audits) of the DPA; and
b) Airia may appoint Sub-Processors under the SCCs as set out in Section 10 (Sub-Processors) of the DPA.

6. **Precedence of SCCs.** If any provision of this SCC Amendment is inconsistent with any terms in the EU SCCs or UK Transfer Addendum (as applicable), the EU SCCs or UK Transfer Addendum (as applicable) shall prevail to the extent of the inconsistency.

7. **Relationship to DPA**. Save as modified by this SCC Amendment, the DPA remains in full force and effect. This SCC Amendment shall be read together with the DPA and the Agreement.

8. **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.

"**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.

"**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 European Data Protection Laws or that has been de-identified within the meaning of European 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 European 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.

"**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.

"**Sub-Processor Table**" the current list of Sub-Processors shown at https://trust.airia.com/subprocessors.

"**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.

Copyright © Airia LLC 2026

By signing below, the Parties agree to be bound by the terms of this SCC Amendment.

AIRIA LLC

Signature: _____

Name: _____

Title: _____

Date: _____

Customer: _____

Signature: _____

Name: _____

Title: _____

Date: _____

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 the 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 this SCC Amendment.
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 the 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 this SCC Amendment.
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

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

Copyright © Airia LLC 2026

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