DATA PROCESSING ADDENDUM

Last Updated: December 22, 2022

This Data Processing Addendum **("DPA")** amends and forms part of the Agreement (as defined below) between Provider and you **("Customer").** Capitalized terms used but not defined below will have the meanings outlined in the Agreement.

1. DEFINITIONS

For purposes of this DPA, the following terms will have the following meaning:

"Agreement" means any agreement between Provider and Customer for the Services. Such an agreement may have various titles, such as "Order Form," "Sales Order," "Terms of Use," "Terms of Service," "SaaS Agreement," or "Services Agreement".

"Controller" has the meaning set forth in GDPR.

"Customer Account and Usage Data" means information about Customer that Customer provides to Provider in connection with the creation and administration of an account, such as first and last name, username, email address, and billing and payment information of individuals associated with an account. This also includes statistical or analytic information related to the Customer's use of the Service and any derived data.

"Customer Data" means information Customer submits for Processing by Provider's Services. This excludes Customer Account and Usage Data.

"Customer Personal Data" means Customer Data which consists of Personal Data.

"Data Protection Law(s)" means any applicable legislation or regulation relating to the processing of personal data, including (a) the California Consumer Privacy Act and its implementing regulations; (b) the GDPR (as defined below) and related data protection and privacy laws of the member states of the European Economic Area; (c) the Data Protection Act 2018 of the United Kingdom ("UK GDPR"); and (d) the Swiss Federal Act on Data Protection ("Swiss DPA"), each as applicable and as amended, repealed, consolidated, or replaced from time to time.

"GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable natural person that Provider processes on behalf of Customer under the Agreement.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"Process" or **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Restricted Transfer" means (a) where the GDPR applies, a transfer of Customer Personal Data or Customer Account and Usage Data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (b) where the Swiss DPA applies, a transfer of Customer Personal Data or Customer Account and Usage Data from Switzerland to a country that is not subject to an adequacy determination by the Swiss Federal Data Protection and Information Commissioner; and (c) where the UK GDPR applies, a transfer of Customer Personal Data or Customer Account and Usage Data from the UK to a country that is not the subject of adequacy regulations under section 17A of the United Kingdom Data Protection Act of 2018.

"Standard Contractual Clauses" means (a) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 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 of the European Parliament and of the Council ("EU SCCs"); (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 ("UK SCCs"); and (c) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs"), each as may be updated from time to time.

2. ROLES OF THE PARTIES

2.1. Customer Personal Data. The parties agree that Provider is a Processor with respect to the Processing of Customer Personal Data.

2.2. Account and Usage Data. The Parties agree that Customer and Provider are independent Controllers with respect to the Processing of Customer Account and Usage Data, and each Party will comply with its obligations as a Controller and agrees to provide reasonable assistance to the other Party when required by Data Protection Laws. With respect to Customer Account and Usage Data, this DPA does not apply except for Section 7.

3. CUSTOMER RESPONSIBILITIES

3.1. Customer agrees that (a) it must comply with its obligations as a Controller under the GDPR and other Data Protection Laws where such concept is recognized in respect of its processing of personal data and any processing instructions it issues to the Provider as referred to in Section 4.1; (b) it has provided notice and obtained all consents and rights required by the Data Protection Laws for the Provider to process Customer Personal Data pursuant to the Agreement and this DPA; and (c) the processing of Customer Personal Data by the Provider in compliance with the documented instructions of Customer under Section 4.1 will have a lawful basis of processing pursuant to Article 6 of the GDPR and other Data Protection Laws that require a lawful basis of processing.

3.2. If Customer is a Processor, Customer represents and warrants to the Provider that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of the Provider as another processor, have been duly authorized by the relevant Controller. Customer must indemnify, defend, and hold the Provider harmless against any claims, actions, proceedings, expenses, damages, and liabilities (including without limitation any governmental investigations, complaints, and actions) and reasonable attorneys' fees arising out of Customer's violation of this Section. Notwithstanding anything to the contrary in the Agreement, Customer's indemnification obligations under this Section will not be subject to any limitations of liability in the Agreement.

4. DATA PROCESSING AND PROTECTION

4.1. Customer instructs Provider to Process Customer Personal Data to provide the Services as documented in the Agreement, unless otherwise required by applicable law. For the avoidance of doubt, this DPA will constitute Customer's documented instructions to the Provider to process Customer's Personal Data in connection with the

Provider's provision of the Service to Customer. Provider must promptly inform Customer if, in the Provider's sole opinion, an instruction violates applicable law.

4.2. Where Provider Processes Customer Personal Data in its capacity as a Processor, it will do so only as necessary to perform the Services. Provider will not "sell" the Customer Personal Data within the meaning of Data Protection Laws. Provider certifies it understands the restrictions of this Section 4.2.

4.3. Provider will use commercially reasonable efforts to ensure that persons authorized by Provider to Process any Customer Personal Data are subject to appropriate confidentiality obligations.

4.4. Provider will, taking into account the nature of the processing, use commercially reasonable efforts to assist Customer, at Customer's expense, by appropriate technical and organizational measures, to the extent possible, in fulfillment of Customer's obligation to respond to requests for exercising the data subjects' rights with respect to their Personal Data under Data Protection Laws.

4.5. At the choice of Customer, Provider will, upon request, delete or return to Customer all Customer Personal Data within thirty (30) days after the end of the provision of the Services to Customer and delete existing copies unless applicable law requires retention of Personal Data.

4.6. Provider will notify Customer promptly if the Provider becomes actually aware of a Personal Data Breach, provided that the provision of such notice or any response by the Provider will not be construed as an acknowledgment of fault or liability with respect to any such Personal Data Breach.

4.7. Provider will use appropriate technical and organizational measures to protect Customer's Personal Data that will meet or exceed the requirements contained (a) under Data Protection Law, and (b) Schedule B to this DPA. Customer acknowledges that the security measures described in Schedule B are subject to technical progress and development and that Provider may update or modify the security measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

5. EU PERSONAL DATA PROCESSING COVENANTS

5.1. Without limitation to Section 4, in processing Personal Data relating to data subjects located in the European Economic Area (including the United Kingdom as of the date of this DPA) ("EU Personal Data"), the following additional terms shall apply:

a) Provider must, taking into account the nature of processing and the information available to the Provider, use commercially reasonable efforts to assist Customer, at Customer's expense, in ensuring compliance with Customer's obligations described in Articles 32 through 36 of the GDPR; and

b) Provider must make available upon Customer's reasonable request information reasonably necessary to demonstrate material compliance with the obligations in this DPA and allow for and contribute to audits (each, an "Audit"), at Customer's expense, including inspections of processing facilities under the Provider's control, conducted by Customer or another auditor chosen by Customer (an "Auditor"), during normal business hours and after reasonable prior notice, provided that no Auditor will be a competitor of the Provider, and provided further that in no event will Customer have access to the information of any other client of the Provider and the disclosures made pursuant to this Section 5.1(b) ("Audit Information") will be held in confidence as the Provider's confidential information and subject to any confidentiality obligations in the Agreement, and provided further that no Audit will be undertaken unless or until Customer has requested, and the Provider has provided, documentation pursuant to this Section and Customer reasonably determines that an Audit remains necessary to demonstrate material compliance with the obligations in this DPA. Without limiting the generality of any provision in the Agreement, Customer must employ the same degree of care to safeguard Audit Information

that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer will be liable for any improper disclosure or use of Audit Information by Customer or its agents.

6. SUBPROCESSORS

6.1. Subprocessors assist the Provider in processing Personal Data as set out in this DPA. The Provider will enter into contractual arrangements with subprocessors requiring the same level of data protection compliance and information security as provided for in this DPA. By entering into the Agreement and this DPA, Customer consents to the processing of Personal Data by, and the disclosure and transfer of Personal Data to, the subprocessors listed at https://www.airslate.com/subprocessors (as updated from time to time in accordance with the DPA). The Provider shall inform Customer via posting an updated list of subprocessors at https://www.airslate.com/subprocessors of any intended changes concerning the addition or replacement of subprocessors at least ten (10) calendar days before the new subprocessor processes EU Personal Data. Customer may object to such changes in writing within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection (an "Objection"). In the event of an Objection, the parties will discuss such concerns in good faith with the intention of achieving a resolution. If the parties are not able to achieve a resolution as described in the previous sentence, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience, on the condition that Customer provides written notice to the Provider within five (5) calendar days of being informed of the engagement of the subprocessor. Customer will not be entitled to any refund of fees paid prior to the date of any termination pursuant to this Section.

7. DATA TRANSFERS

7.1. Customer consents to the transfer of EU Personal Data to, and the processing of EU Personal Data in, the United States of America.

7.2. Transfers from the EEA. Where a Restricted Transfer is made from the EEA, the EU SCCs are incorporated into this DPA and apply to the transfer as follows:

a) with respect to Restricted Transfers from Customer to Provider, Module One applies where both Customer and Provider are Controllers, Module Two applies where Customer is a Controller and Provider is a Processor, and Module Three applies where both Customer and Provider are Processors;

b) in Clause 7, the optional docking clause does not apply;

c) in Clause 9 of Modules Two and Three, Option 2 applies, and the period for prior notice of subprocessor changes is specified in Section 6 of this DPA;

d) in Clause 11, the optional language does not apply;

e) in Clause 17, Option 1 applies with the governing law that is designated in the *Choice of Law; Venue* section of the Agreement. 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; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales;

f) in Clause 18(b), disputes will be resolved before the courts in the applicable venue of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the courts of England and Wales will have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses.

For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes;

g) Annex I of the SCCs is completed with the information in Schedule A to this DPA; and

h) Annex II of the SCCs is completed with the information in Schedule B to this DPA; and Annex III of the SCCs is completed with the information in the Subprocessors List.

7.3. Transfers from Switzerland. In case of any transfers of Data from Switzerland, (a) general and specific references in the EU SCCs to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Swiss DPA, as applicable; and (b) any other obligation in the EU SCCs determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under Swiss DPA, as applicable.

7.4. Transfers from the UK. Where a Restricted Transfer is made from the UK, the UK Transfer Addendum is incorporated into this DPA and applies to the transfer. The UK Transfer Addendum is completed with the information in Section 7.2, the Subprocessors List, and Schedules A and B to this DPA; and both "Importer" and "Exporter" are selected in Table 4.

7.5. If Provider adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to Data Protection Law) for the transfer of personal data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism will apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Law and extends to the territories to which Personal Data is transferred).

8. MISCELLANEOUS

8.1. The terms of this DPA will control to the extent there is any conflict between terms of this DPA and the terms of the Agreement. If there is any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail with respect to EU, Swiss, or UK Personal Data. Except as specifically amended and modified by this DPA, the terms and provisions of the Agreement remain unchanged and in full force and effect. Except as outlined in Section 3 of this DPA, the obligations contained in this DPA are (a) subject to any limitations of liability outlined in the Agreement, and (b) in addition to the other obligations contained in the Agreement. This DPA may be executed electronically, including using Provider's electronic signature Services.

Provider	**Customer**
Signature: Roman Perchyts	**Signature:** Bradley Dizonno Verified by airSlate inc. 11/09/23 17:10 UTC 45C9E09D-C400006F
By: Roman Perchyts	**By:** Bradley Dizonno
Title: General Counsel	**Title:** Director of Technology and Analytics
Date: 09/21/2023	**Date:** 11/09/2023

SCHEDULE A – Details of Processing

Section A: List of Parties

Data Importer: Provider	**Data Exporter**: Customer
Address: Contracting Entity **Contact Person's Name:** *N/A* **Position:** General Counsel **Contact**: privacy@airslate.com **Role**: Processor/Controller	**Address**: 590 Medinah Road , Roselle 60172, United States of America **Contact Person's Name:** Bradley Dizonno **Position:** Director of Technology and Analytics **Contact**: bdizonno@lphs.org **Role**: Controller

Section B: Description of Processing/Transfer

- **Categories of data subjects whose personal data is transferred**

  Representatives of Customer; representatives of partners; Services users and Services visitors, including without limitation recipients of files uploaded into the Services; and individuals referenced in files uploaded into the Services.

- **Categories of personal data transferred**

  EU Personal Data relating to the category of data subjects described above. The EU Personal Data depends on the particular Services but could include: Name, email address, IP address, employer, address, telephone number, occupation, and position, and any EU Personal Data provided by Customer and Services users and Services visitors (including without limitation recipients of files uploaded into the Services) in connection with the Services, including Customer Personal Data contained within files uploaded into the 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

  The contents of the Personal Data are varied and under the data exporter's control, but may, from time to time, depending on the particular Services, include sensitive data under the relevant Data Protection Laws.

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

  Transfers will be continuous for the duration necessary for the performance of the Services; any other purposes stipulated in the Agreement; and complying with applicable laws and regulations.

- **Nature of the processing**

  The EU Personal Data will be subject to basic processing, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction for the purpose of providing Services by the Provider to Customer in accordance with the terms of the Agreement.

- **Purpose(s) of the data transfer and further processing**

  EU Personal Data will be subject to those Processing operations described in 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**

  In the course of providing such Services to Customer, Provider will, for the duration of the Agreement, Process EU Personal Data as instructed by Customer.

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

  All authorized sub-processors are required to implement and maintain the same or substantially similar technical and organizational measures, responsibilities, and obligations as those required of Provider under this DPA.

Section C: Competent Supervisory Authority

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

- Where the data exporter 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 will act as the competent supervisory authority.

- Where the data exporter 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: Data Protection Commission (DPC) – 21 Fitzwilliam Square, South Dublin 2, D02 RD28 Ireland will act as the competent supervisory authority.

- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office will act as the competent supervisory authority.

- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner will act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

SCHEDULE B – Security Measures

1. **Program.** Provider will implement and maintain a written information security program ("Information Security Program"), which contains reasonably appropriate administrative, technical, and organizational safeguards that comply with this Schedule.

2. **Access Controls.** Provider will implement measures to: (a) abide by the "principle of least privilege," pursuant to which access to Personal Data by Provider personnel will be limited on a need-to-know basis; and (b) promptly terminate its personnel's access to Personal Data when such access is no longer required for performance under the Agreement.

3. **Account Management.** Provider will manage the creation, use, and deletion of all account credentials used to access the Provider's key infrastructure, including by requiring multi-factor authentication in all critical systems.

4. **Vulnerability Management.** Provider will: (a) periodically use automated vulnerability scanning tools to scan the Provider's production system for vulnerabilities, including but not limited to penetration testing; and (b) implement patch management and software update tools as notified by the providers of those tools.

5. **Security Segmentation.** Provider will monitor, detect and restrict the flow of information on a multilayered basis using tools such as firewalls, proxies, and network-based intrusion detection systems.

6. **Data Loss Prevention.** Provider will use loss prevention measures to identify, monitor, and protect Personal Data in use, in transit, and at rest. Such data loss prevention processes and tools will include: (a) automated tools designed to identify attempts of data exfiltration; and (b) the use of encryption certificate-based security.

7. **Encryption.** Provider will encrypt, using industry-standard encryption tools, all Personal Data that Provider transmits across public networks.

8. **Pseudonymization.** Provider will, where possible and consistent with the Services, use industry-standard pseudonymization techniques to protect Personal Data.

9. **Physical Safeguards.** Provider will maintain physical access controls to secure the Provider-owned physical premises where the relevant Provider computing environment used to Process any Personal Data is located, including an access control system that enables Provider to control physical access to each Provider facility.

10. **Administrative Safeguards.** Prior to providing access to Customer Personal Data to any of its personnel, Provider will use commercially reasonable measures: (a) verify the reliability of such personnel; and (b) provide appropriate security training to such personnel.