DATA PROCESSING ADDENDUM

Argus PBI LLC

Effective Date: [Date of publication]

This Data Processing Addendum ("Addendum" or "DPA") is incorporated into and forms part of the agreement between **Argus PBI LLC** ("Processor" or "Argus") and the customer that has accepted the Argus Terms of Service or signed another written agreement with Argus for the Services (that agreement, the "applicable agreement") ("Customer" or "Controller") (collectively, the "Parties"). This Addendum takes effect when Customer accepts or signs the applicable agreement, without a separate signature.

This Addendum governs the Processing of Personal Data by Argus on behalf of Customer in connection with the services provided under the applicable agreement ("Services").

1. DEFINITIONS

For purposes of this Addendum:

1.1. "Applicable Data Protection Laws" means all applicable privacy and data protection laws and regulations governing the Processing of Personal Data under this Addendum, including, where applicable, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), the EU General Data Protection Regulation ("GDPR"), and the UK GDPR.

1.2. "Controller" means the entity that determines the purposes and means of Processing Personal Data. Under this Addendum, Customer is the Controller.

1.3. "Processor" means the entity that Processes Personal Data on behalf of the Controller. Under this Addendum, Argus PBI LLC is the Processor.

1.4. "Personal Data" means any information relating to an identified or identifiable natural person that is Processed by Argus on behalf of Customer under the applicable agreement, and includes "personal information" as defined in the CCPA.

1.5. "Processing" means any operation or set of operations performed on Personal Data, including collection, access, storage, use, disclosure, transmission, alteration, retrieval, or deletion.

1.6. "Subprocessor" means any third party engaged by Argus to Process Personal Data on behalf of Customer in connection with the Services.

1.7. "Data Subject" means an identified or identifiable natural person whose Personal Data is Processed under this Addendum.

1.8. "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 Processed by Argus on behalf of Customer.

1.9. "Standard Contractual Clauses" means the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), and **"UK Addendum"** means the International Data Transfer Addendum to those clauses issued by the UK Information Commissioner.

2. ROLES AND RESPONSIBILITIES

2.1. Controller Responsibilities. Customer acts as the Controller of Personal Data and is responsible for determining the purposes and means of Processing. Customer represents and warrants that it has all necessary rights, permissions, notices, and lawful bases required to provide Personal Data to Argus for Processing.

2.2. Processor Responsibilities. Argus acts as the Processor and shall Process Personal Data only on documented instructions from Customer, including as necessary to provide the Services, comply with the applicable agreement, and fulfill the obligations set forth in this Addendum, unless applicable law requires otherwise, in which case Argus shall inform Customer of that legal requirement before Processing unless the law prohibits it. The applicable agreement, this Addendum, and Customer's configuration of the Services and of Argus's access in Customer's Microsoft tenant are Customer's complete documented instructions.

2.3. No Independent Use. Argus shall not sell Personal Data or retain, use, or disclose Personal Data for purposes other than performing the Services or as otherwise permitted by Applicable Data Protection Laws and this Addendum.

2.4. Customer Instructions. Customer is responsible for ensuring that its Processing instructions comply with Applicable Data Protection Laws. Argus shall notify Customer if, in Argus's reasonable opinion, an instruction violates Applicable Data Protection Laws, unless prohibited by law.

3. PROCESSING OF PERSONAL DATA

3.1. Scope and Purpose. Argus shall Process Personal Data solely to provide, maintain, secure, and support the Services as authorized by Customer and as described in Schedule 1, the applicable agreement, and this Addendum.

3.2. Categories of Data. Depending on the Services and Customer's use, Personal Data may include business contact information, account information, user identifiers, IP addresses, user agent strings, activity records, access rights, communications, and other information submitted or made available by Customer, as further described in Schedule 1.

3.3. Categories of Data Subjects. Data Subjects may include Customer's employees, contractors, representatives, business contacts, authorized users, and other individuals whose Personal Data Customer submits or makes available through the Services.

3.4. Duration. Argus shall Process Personal Data for the duration of the applicable agreement and thereafter until it is returned or deleted under Section 8, subject to any retention or deletion obligations set forth in this Addendum or required by law.

3.5. Processing Records. Argus shall maintain records of Processing activities to the extent required by Applicable Data Protection Laws.

4. CONFIDENTIALITY AND SECURITY

4.1. Confidentiality. Argus shall ensure that personnel authorized to Process Personal Data are subject to appropriate confidentiality obligations.

4.2. Security Measures. Argus shall implement and maintain reasonable administrative, technical, and organizational safeguards designed to protect Personal Data against unauthorized access, disclosure, alteration, loss, or destruction.

4.3. Security Controls. Such safeguards include the measures described in Schedule 2, which Argus may update from time to time provided that an update does not materially

reduce the overall protection of Personal Data, and may also include, as appropriate to the nature of the Services and Personal Data:

- Access controls and authentication measures.
- Appropriate encryption and secure transmission practices.
- Personnel confidentiality and security awareness measures.
- Security monitoring and incident response procedures.
- Reasonable measures to protect systems and infrastructure.
- Secure deletion and disposal practices.

4.4. Security Reviews. Argus shall periodically review its security measures and make reasonable updates to address relevant risks and changes in technology.

5. PERSONAL DATA BREACHES

5.1. Notification. Argus shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of Customer, and shall use reasonable efforts to do so within seventy-two (72) hours after confirming the Personal Data Breach. For purposes of this Section 5, a compromise of a credential that Argus uses to access Customer's Microsoft environment is treated as a Personal Data Breach, whether or not Argus has confirmed that Personal Data was accessed.

5.2. Breach Information. To the extent reasonably available, Argus shall provide information concerning the nature of the breach, the categories of Personal Data affected, the likely consequences, and the measures taken or proposed to address the breach.

5.3. Cooperation. Argus shall reasonably cooperate with Customer in investigating, mitigating, and addressing the breach and in fulfilling applicable legal notification obligations.

5.4. Responsibility for Notifications. Customer, as Controller, is responsible for determining whether notifications to Data Subjects, regulators, or other parties are required, except to the extent applicable law imposes a direct obligation on Argus.

5.5. No Admission. Argus's notification of or response to a Personal Data Breach is not an acknowledgment of fault or liability.

6. SUBPROCESSORS

6.1. Authorization. Customer authorizes Argus to engage Subprocessors as reasonably necessary to provide the Services, including the Subprocessors listed in Schedule 3.

6.2. Subprocessor Obligations. Argus shall impose data protection obligations on its Subprocessors that are substantially equivalent to the applicable obligations under this Addendum.

6.3. Responsibility. Argus shall remain responsible for its Subprocessors' performance of their data protection obligations to the extent required by Applicable Data Protection Laws.

6.4. Changes to Subprocessors. Argus shall provide at least thirty (30) days' notice of any new Subprocessors (by email or by updating Schedule 3 with notice to Customer) and give Customer a reasonable opportunity to raise a substantiated objection on data protection grounds. If the Parties cannot resolve an objection, Customer may terminate the applicable agreement as its sole remedy, and Argus shall refund any prepaid fees for the period after termination.

7. DATA SUBJECT RIGHTS

7.1. Assistance. Taking into account the nature of the Processing, Argus shall provide reasonable assistance to Customer, through appropriate technical and organizational measures where feasible, to enable Customer to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Laws.

7.2. Direct Requests. If Argus receives a request directly from a Data Subject concerning Personal Data Processed on behalf of Customer, Argus shall, where legally permitted, direct the Data Subject to Customer and promptly notify Customer of the request.

7.3. No Independent Determination. Argus shall not independently determine whether a Data Subject request should be granted, except where required by law or where the request relates to data Argus Processes in an independent capacity.

8. DATA RETENTION AND DELETION

8.1. Retention. Argus shall retain Personal Data only for as long as reasonably necessary to provide the Services or as otherwise required by the applicable agreement or law.

8.2. Deletion or Return. Upon termination or expiration of the applicable agreement, Argus shall, at Customer's choice and subject to applicable legal requirements, return or delete Personal Data in its possession or control. Customer may request return, in the form of the export described in the Argus Privacy Policy, within thirty (30) days after termination or expiration. Argus shall complete deletion within thirty (30) days after Customer's written request, and in any event no later than the end of the retention period in Section 8.5, and shall confirm deletion in writing on request.

8.3. Backup Copies. Personal Data contained in routine backup systems may be retained for a limited period in accordance with Argus's standard backup retention procedures, provided that such data remains protected under this Addendum and is not restored or otherwise Processed except as necessary for disaster recovery, security, or legal compliance.

8.4. Legal Retention. If Argus is required by law to retain Personal Data, Argus shall inform Customer of that requirement where legally permitted and shall continue to protect the retained data in accordance with this Addendum.

8.5. Standard Retention. Argus retains Personal Data collected from Customer's Microsoft environment for twelve (12) months from collection, after which it is deleted automatically, subject to a recovery period of up to seven (7) days in Argus's storage provider before permanent removal. Customer instructs Argus to apply this retention period.

9. INTERNATIONAL DATA TRANSFERS

9.1. Transfers. Argus shall not transfer Personal Data to a country outside the jurisdiction in which it was collected except as authorized by Customer or as otherwise permitted by Applicable Data Protection Laws. Customer authorizes Argus to Process Personal Data in the United States, including by remote access by Argus personnel located in the United States to Personal Data stored in another jurisdiction, and in the locations of the Subprocessors listed in Schedule 3.

9.2. Transfer Safeguards. Where applicable law requires safeguards for international transfers, the Parties shall cooperate in implementing appropriate safeguards, which may include standard contractual clauses or other legally recognized transfer mechanisms.

9.3. EU and UK Transfers. To the extent Customer's transfer of Personal Data to Argus is subject to the GDPR or the UK GDPR, the Standard Contractual Clauses are incorporated

into this Addendum by reference, with Customer as data exporter and Argus as data importer, and are completed as follows: Clause 7 (docking clause) applies; under Clause 9, Option 2 (general written authorization) applies, with the notice period in Section 6.4; the optional wording in Clause 11 does not apply; under Clauses 17 and 18, the law and courts of Ireland apply; and Annexes I and II are completed by Schedules 1 and 2. For transfers subject to the UK GDPR, the UK Addendum applies, with its tables completed using the information in this Addendum and Schedules 1 through 3. If there is a conflict between the Standard Contractual Clauses or the UK Addendum and this Addendum or the applicable agreement, the Standard Contractual Clauses or the UK Addendum control.

10. AUDITS AND COMPLIANCE

10.1. Compliance Information. Upon reasonable written request, Argus shall make available information reasonably necessary to demonstrate its compliance with the data protection obligations applicable to it under this Addendum.

10.2. Audits. Where required by Applicable Data Protection Laws, Customer may conduct or appoint an independent auditor to conduct a reasonable audit of Argus's relevant Processing activities, subject to at least thirty (30) days' advance notice, confidentiality obligations, and safeguards to protect the security and confidentiality of Argus's systems and other customers' information. Audits may occur no more than once in any twelve (12) month period, except following a Personal Data Breach or at the direction of a supervisory authority, and only where the information made available under Section 10.1 is not reasonably sufficient to demonstrate compliance.

10.3. Audit Limitations. Audits shall be conducted during normal business hours, shall not unreasonably disrupt Argus's operations, and shall be limited to information and systems relevant to the Processing of Customer's Personal Data.

10.4. Audit Costs. Unless otherwise required by law or the applicable agreement, Customer shall bear the costs of audits it requests.

11. REGULATORY COOPERATION

Argus shall provide reasonable cooperation to Customer, taking into account the nature of the Processing and information available to Argus, in connection with regulatory inquiries, data protection impact assessments, and consultations with supervisory authorities where required by Applicable Data Protection Laws.

12. CALIFORNIA PRIVACY REQUIREMENTS

To the extent the CCPA applies to the Processing of Personal Data under this Addendum:

12.1. Service Provider or Contractor. Argus shall act as a service provider or contractor, as applicable under the CCPA, with respect to Personal Information Processed on behalf of Customer.

12.2. Permitted Purposes. Argus shall Process Personal Information only for the limited and specified business purposes set forth in Schedule 1, consistent with the applicable agreement and this Addendum.

12.3. Prohibited Uses. Argus shall not:

- Sell or share Personal Information as those terms are defined under the CCPA.
- Retain, use, or disclose Personal Information for any purpose, including any commercial purpose, other than the business purposes specified in Schedule 1, except as permitted by the CCPA.
- Retain, use, or disclose Personal Information outside the direct business relationship between Argus and Customer, except as permitted by the CCPA.
- Combine Personal Information received from Customer with Personal Information received from other sources except as permitted by the CCPA.
- Use Personal Information in a manner inconsistent with the applicable contractual restrictions and legal requirements.

12.4. Compliance Assistance. Argus shall comply with its applicable obligations under the CCPA, provide the same level of privacy protection as the CCPA requires of Customer, and provide reasonable assistance to Customer in meeting applicable CCPA obligations, and shall promptly notify Customer if Argus determines it can no longer meet its applicable obligations under the CCPA.

12.5. Verification and Remediation. Customer may take reasonable and appropriate steps to verify that Argus uses Personal Information consistently with Customer's obligations under the CCPA and may require Argus to take reasonable steps to stop and remediate unauthorized use.

13. LIABILITY

Each Party's liability arising out of or relating to this Addendum shall be subject to the limitations, exclusions, and allocation of liability set forth in the applicable agreement, and any liability under this Addendum counts toward, and is not in addition to, the aggregate limitation of liability in the applicable agreement. This Addendum does not create any indemnification obligation or any separate or additional limitation of liability. Nothing in this Section 13 limits either Party's liability to Data Subjects under the Standard Contractual Clauses where they apply, or limits liability between the Parties to the extent the Standard Contractual Clauses do not permit it.

Nothing in this Addendum shall exclude or limit liability where such exclusion or limitation is prohibited by applicable law.

14. TERM AND TERMINATION

14.1. Term. This Addendum shall remain in effect for the duration of the applicable agreement, unless terminated earlier in accordance with that agreement.

14.2. Survival. Obligations relating to confidentiality, security, retention, deletion, and any other provisions that by their nature should survive termination shall continue to apply for as long as Argus retains or Processes Personal Data on behalf of Customer.

15. GENERAL PROVISIONS

15.1. Order of Precedence. In the event of a conflict between this Addendum and the applicable agreement concerning the Processing of Personal Data, this Addendum shall control to the extent of the conflict, except that Section 13 of this Addendum and the limitations and exclusions of liability in the applicable agreement control over any other provision of this Addendum, unless the Parties expressly agree otherwise in writing.

15.2. Amendments. Any amendment to this Addendum must be made in writing and agreed to by both Parties, except for updates permitted under the applicable agreement or required by law, and updates Argus makes on at least thirty (30) days' notice that do not materially reduce the protection of Personal Data.

15.3. Governing Law. This Addendum shall be governed by the governing law provision of the applicable agreement, unless otherwise required by Applicable Data Protection Laws.

15.4. Entire Agreement. This Addendum, together with the applicable agreement, constitutes the entire agreement between the Parties concerning the Processing of Personal Data covered by this Addendum.

SIGNATURES

The Parties acknowledge that they have read, understood, and agree to the terms of this Data Processing Addendum. A signature is not required for this Addendum to take effect. Customers that require a countersigned copy may complete the signature block below and send it to **info@arguspbi.com.**

CUSTOMER (CONTROLLER)

Legal Name: _____

By: _____

Title: _____

Date: _____

ARGUS PBI LLC (PROCESSOR)

By: _____

Title: _____

Date: _____

SCHEDULE 1: DESCRIPTION OF PROCESSING

Subject matter and nature. Argus reads metadata and activity information from Customer's Microsoft Power BI and Microsoft Fabric environments through Microsoft's

read-only admin APIs, using access that Customer's administrator authorizes in Customer's Microsoft tenant, and stores, analyzes, and presents that information to Customer through the Services.

Business purposes. (a) Monitoring dataset refreshes and alerting Customer to failures; (b) providing insights into user activity and access rights; (c) mapping data lineage and dependencies; (d) providing exports of Customer's historical information on request; and (e) providing customer support and securing, maintaining, and troubleshooting the Services.

Categories of Data Subjects. Customer's employees, contractors, guest users, and other individuals who have access to, or activity in, Customer's Power BI or Fabric environment, including individuals who request dataset refreshes.

Categories of Personal Data. Display names; email addresses and user principal names; user IDs and user type; client IP addresses; user agent strings; activity records (the action taken, the item affected, and the date and time); access rights to workspaces, datasets, and reports; the identity of individuals who request dataset refreshes; and any Personal Data that appears in item names or descriptions, query definitions (DAX and Power Query (M) expressions), connection details (such as server names and file paths), or data entered directly into a dataset.

Sensitive data. None is intended to be Processed. Customer should not include sensitive data, passwords, keys, or tokens in item names, query definitions, or connection details.

Frequency. Continuous, on a scheduled basis while the Services are active.

Retention. As described in Section 8.

Location. Microsoft Azure in the United States or, for customers in the European Union, an Azure region in the European Union, with remote access by Argus personnel located in the United States.

Competent supervisory authority. Where the Standard Contractual Clauses apply, as determined under Clause 13 of those clauses.

SCHEDULE 2: SECURITY MEASURES

Access control. Access to Argus systems and to Customer's Personal Data is limited to a small number of authorized personnel who need it to provide the Services, and requires multi-factor authentication.

Least privilege in Customer's tenant. Argus requests read-only access to Power BI and Fabric admin APIs. Argus does not connect to Customer's underlying data sources and does not hold credentials to them.

Credential protection. Argus stores the credentials its application uses to access Customer tenants in a managed secrets vault, restricts access to them to authorized personnel, and rotates them periodically.

Encryption. Data in transit is encrypted using HTTPS/TLS. Data at rest is encrypted by Microsoft Azure storage encryption.

Segregation. Each customer's service data is stored in a separate storage container.

Personnel. Personnel and service providers with access to Personal Data are bound by written confidentiality obligations.

Retention and deletion. Service data is deleted automatically after twelve (12) months, and on Customer's request as described in Section 8.

Incident response. Argus maintains a written data breach response plan and follows the notification commitments in Section 5.

SCHEDULE 3: SUBPROCESSORS

Microsoft Corporation (Microsoft Azure). Hosting and storage of all service data. Location: United States; for customers in the European Union, an Azure region in the European Union.