DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("DPA") forms part of the Master Services Agreement ("Agreement") between **[Client Company Name]**, acting as the Data Controller ("Controller"), and **Arvoan Ltd** (officially registered in Finland as Arvoan Oy, Business ID: 3286668-5) **(Toni Ruokolainen)**, acting as the Data Processor ("Processor").

This DPA governs the processing of Personal Data under the European Union General Data Protection Regulation (GDPR) in connection with the Revenue Architecture services provided by the Processor.

1. Scope and Roles

1.1. The Controller appoints the Processor to process Personal Data on behalf of the Controller.
1.2. The subject matter, nature, purpose, and duration of the processing, as well as the types of Personal Data and categories of Data Subjects, are outlined in **Annex I** of this DPA.

2. Processor Obligations

2.1. **Instructions:** The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by European Union or Member State law.
2.2. **Confidentiality:** The Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality.
2.3. **Data Minimization & PII Scrubbing:** Upon ingestion of the data into the Processor's secure local environment, the Processor will execute a data minimization protocol to flag and remove non-essential Personally Identifiable Information (e.g., cleartext names) before exploratory statistical analysis begins.

3. Security of Processing (The Zero-Trust Protocol)

3.1. Taking into account the state of the art and the risks presented by processing, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
3.2. **Encrypted Clean Room:** The Processor transfers data from the Controller’s systems solely via encrypted, audit-logged pipelines. All downloaded Controller Data is strictly isolated utilizing "Cryptographic Compartmentalization" on dedicated Linux LUKS2 partitions.

3.3. Further details on the specific Technical and Organizational Measures (TOMs) are specified in **Annex II**.

4. Sub-processing

4.1. The Controller grants the Processor general authorization to engage Sub-processors.
4.2. The current list of approved Sub-processors is set out in **Schedule 3**. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller the opportunity to object.
4.3. The Processor remains fully liable to the Controller for the performance of the Sub-processor's obligations.

5. Personal Data Breaches

5.1. The Processor shall notify the Controller without undue delay, and **no later than 24 hours** after becoming aware of a Personal Data breach. The notification shall describe the nature of the breach and the measures taken to address it.

6. Return and Cryptographic Erasure of Data

6.1. Upon termination of the Agreement or completion of the specific Sprint, the Processor shall execute a "Leave No Trace" protocol.
6.2. Instead of standard file deletion, the Processor shall completely destroy the specific encrypted container file housing the Controller's data, which mathematically destroys the cryptographic header and master key, rendering the underlying data forensically unrecoverable.

7. Audit Rights & Compliance

7.1. **General Audit Right:** The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR.
7.2. **The "Questionnaire-First" Principle:** To minimize disruption to the Processor's business operations, the Controller agrees to exercise its audit right by first requesting written responses to reasonable security questionnaires or requesting documentation of the Processor's security protocols.
7.3. **Audit Conditions:** If a formal audit or inspection is deemed strictly necessary beyond

written documentation, it shall be subject to the following conditions:

- **Notice:** The Controller must provide at least thirty (30) days' prior written notice.
- **Frequency:** Audits are limited to once per calendar year, unless a confirmed Personal Data breach has occurred.
- **Confidentiality & Physical Access:** Because the Processor utilizes shared or private facilities, physical on-site inspections of the Processor's premises are strictly prohibited unless mandated by law. Audits will be conducted remotely via screen-share, log review, or video conference to verify encryption configurations and data destruction protocols.
- **Costs:** The Controller shall bear all costs and expenses associated with conducting the audit, including compensating the Processor at their standard hourly consulting rate for time spent assisting with the audit.

8. International Transfers

8.1. If the Processor processes or transfers Personal Data outside the European Economic Area (EEA), it shall ensure that such transfers are protected by appropriate safeguards (e.g., EU Standard Contractual Clauses or a recognized Adequacy Decision).

9. Miscellaneous and Electronic Signatures

9.1. **Governing Law:** This DPA and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of **Finland**, without giving effect to any choice or conflict of law provision or rule.
9.2. **Severability:** If any provision of this Agreement is held to be invalid, illegal, or unenforceable, the other provisions shall remain in full force and effect.
9.3. **Electronic Signatures:** The Parties agree that this Agreement may be signed electronically. Electronic signatures (including those provided via PandaDoc, DocuSign, or similar platforms) shall have the same legal validity and enforceability as a handwritten signature. The Parties agree that the audit trail provided by the electronic signature platform shall suffice as proof of signature.

ANNEX I: DETAILS OF PROCESSING

A. Nature and Purpose of Processing:
To analyze product usage events, establish Go-To-Market baselines, calculate account health scores, correlate product behavior with revenue outcomes, and deploy data architecture models (e.g., dbt packages) into the Controller's data warehouse. Data downloaded locally is strictly for exploratory statistical analysis and process mining.

B. Duration of Processing:
Processing will occur strictly for the duration of the active Sprint (e.g., 1 to 4 weeks) as defined in the applicable Order Form or MSA, after which all local data will be cryptographically destroyed.

C. Categories of Data Subjects:
End-users of the Controller's SaaS platform and employees of the Controller's customers.

D. Types of Personal Data:
Product usage telemetry, timestamps, IP addresses, user_id, anonymous_id, and context_group_id (Account ID). Additionally, email addresses, subscription tiers, and financial labeling data (e.g., Stripe billing events, CRM exports) required for revenue correlation.
(Note: Full credit card numbers, bank account details, or raw payment instruments are explicitly out of scope, are not required for analysis, and should never be transferred to the Processor).

ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

The Processor implements the following security architecture to ensure the confidentiality, integrity, and isolation of the Controller's data:

1. Secure Ingestion & Transit:

- **Primary Route (Scoped API):** Direct, read-only API connections to the Controller's data warehouse (e.g., GCP Service Account) and revenue systems (e.g., restricted Stripe API keys). Data is transferred in transit using TLS 1.2 or higher (TLS 1.3 preferred).
- **Secondary Route (Drop Zone):** For offline data transfers, a provisioned, access-controlled cloud folder (Google Workspace) protected by AES-256 encryption at rest and TLS in transit.

2. Cryptographic Compartmentalization (Local Storage):

- **Dedicated Encrypted Containers:** Customer Data is never stored directly on the host file system. Instead, it is stored strictly within dedicated, file-based **LUKS2 (Linux Unified Key Setup)** encrypted .img containers using the **AES-256 (XTS-plain64)** cipher specification.
- **One Client, One Vault:** A separate, isolated container file is created exclusively for the Controller. Cross-contamination between clients is prevented by architectural design.
- **Key Management:** Containers are secured with high-entropy passphrases stored in an industry-standard encrypted password manager (1Password). Decryption keys are never stored in plain text or code repositories.

3. Workstation Security & Isolation:

- **Host Isolation:** The host operating system (Fedora Linux) is hardened with SELinux (Security-Enhanced Linux) in Enforcing mode.
- **Memory Protection:** Disk-based swap memory is encrypted (via ZRAM) to prevent the leakage of unencrypted data fragments to the physical disk.
- **Workspace Containment:** Analytical tools (e.g., Python, Polars) run within the context of the mounted encrypted container. Temporary files and caches are directed to the encrypted volume to prevent data leakage to the host OS.

4. Data Erasure:

- Upon termination of services, the specific LUKS container file associated with the Controller is deleted. This destroys the cryptographic header and master key, instantly rendering the underlying data mathematically irrecoverable.

SCHEDULE 3: LIST OF SUB-PROCESSORS

The Controller agrees to the Processor's use of the following Sub-processors to process Personal Data:

Sub-processor Name	**Corporate Location**	**Description of Processing**	**Location of Data**
Google Cloud Platform (Google LLC)	USA	Cloud storage (Google Drive "Drop Zone"), data warehousing (BigQuery API integration).	EU / Finland
1Password (AgileBits Inc.)	Canada	Management of encryption keys and credentials. *(Note: Only processes credentials, not Customer Data contents).*	Canada / USA
PandaDoc, Inc.	USA	Electronic signature execution and contract lifecycle management. *(Note: Only processes contact details and audit trails for contract execution, not raw product telemetry).*	USA (Subject to EU Standard Contractual Clauses)

SIGNATURES

By signing below, the authorized representatives of the Parties agree to be bound by this Data Processing Agreement.

For the Data Controller [Client Company]:
Name: _____
Title: _____
Date: _____
Signature: _____

For the Data Processor (Arvoan Ltd):
Name: Toni Ruokolainen
Title: B2B Revenue Architect
Date: _____
Signature: _____