DATA PROCESSING AGREEMENT (DPA)

Between: Denev Operations LTD, ("Processor") and **Customer**, ("Controller")

Last Updated: 02/03/2026 (dd/mm/yyyy)

This Data Processing Agreement ("Agreement" or "DPA") forms part of the Terms of Service or other written or electronic agreement ("Principal Agreement") between **Denev Operations LTD** ("Processor") and the entity or individual using the Processor's Services ("Controller").

This DPA governs the Processing of Personal Data by Processor on behalf of Controller in connection with the provision of the Processor's SaaS automation and workflow platform ("Service").

1. Definitions

For the purposes of this DPA:

- **"Personal Data"** means any information relating to an identified or identifiable natural person.
- **"Processing"** means any operation performed on Personal Data, automated or otherwise.
- **"Controller"** means the entity determining the purposes and means of Processing.
- **"Processor"** means the entity Processing Personal Data on behalf of the Controller.
- **"Sub-Processor"** means any third party engaged by Processor to Process Personal Data.
- **"Applicable Data Protection Laws"** means all laws relating to data protection, privacy, and security, including GDPR, UK GDPR, CCPA (where applicable), PIPEDA, and the Australian Privacy Act.
- **"Standard Contractual Clauses (SCCs)"** means the EU Commission's approved clauses for international data transfers.
- **"Service Data"** means Personal Data processed through the Service.
- **"User-Generated Content"** means workflows, automations, files, and other data uploaded or created by Controller.

2. Roles of the Parties

2.1 Controller

Controller determines the purposes and means of Processing Personal Data.

2.2 Processor

Processor Processes Personal Data solely on behalf of Controller and in accordance with Controller's documented instructions.

2.3 Nature of Processing

Processor provides a cloud-based automation and workflow platform that stores, executes, and manages workflows and related data.

3. Subject Matter, Duration, and Purpose of Processing

3.1 Subject Matter

Processing of Personal Data submitted by Controller through the Service.

3.2 Duration

This DPA remains in effect for as long as Processor Processes Personal Data on behalf of Controller.

3.3 Purpose

To provide, maintain, secure, and improve the Service.

4. Categories of Data Subjects and Personal Data

4.1 Data Subjects

- Controller's customers
- Controller's employees or contractors
- End-users interacting with Controller's workflows
- Any individuals whose data is included in User-Generated Content

4.2 Categories of Personal Data

- Name
- Email address
- Address
- Country
- Postal code

- Tax Identification Number (TIN)
- Workflow data and User-Generated Content
- Uploaded files
- Technical logs and metadata
- IP addresses and device information

Processor does **not** intentionally process special categories of data (GDPR Art. 9).

5. Processor Obligations

Processor shall:

5.1 Process Only on Documented Instructions

Process Personal Data only:

- As necessary to provide the Service
- As documented by Controller
- As required by law

5.2 Confidentiality

Ensure all personnel authorized to Process Personal Data are bound by confidentiality obligations.

5.3 Security Measures

Implement appropriate technical and organizational measures, including:

- Encryption at rest and in transit
- Access controls and authentication
- Network segmentation
- Encrypted in-memory sandbox environments
- Regular security assessments
- Audit logging

5.4 Assistance to Controller

Processor shall assist Controller in:

- Responding to Data Subject requests

- Conducting Data Protection Impact Assessments (DPIAs)
- Managing consultations with supervisory authorities

5.5 Data Breach Notification

Notify Controller **without undue delay** after becoming aware of a Personal Data Breach.

Notification will include:

- Nature of the breach
- Categories and approximate number of Data Subjects affected
- Likely consequences
- Measures taken or proposed

5.6 Deletion or Return of Data

Upon termination of the Service, Processor shall:

- Delete all Personal Data from active systems
- Delete or return Personal Data upon written request
- Remove Personal Data from backups according to standard rotation schedules

6. Controller Obligations

Controller shall:

- Ensure it has a lawful basis for Processing
- Not upload unlawful or prohibited data
- Configure the Service securely
- Maintain accuracy of Personal Data
- Comply with all Applicable Data Protection Laws

7. Sub-Processors

7.1 Authorized Sub-Processors

Controller authorizes Processor to use the following Sub-Processors:

Sub-Processor	Purpose	Location
OVH	Cloud hosting	EU/Canada
Wasabi	Object storage	USA/EU
Stripe	Payment processing	Global

7.2 Sub-Processor Obligations

Processor shall:

- Enter into written agreements with Sub-Processors

- Ensure Sub-Processors provide equivalent data protection
- Remain fully liable for Sub-Processor actions

7.3 Changes to Sub-Processors

Processor will notify Controller of changes and provide an opportunity to object on reasonable grounds.

8. International Data Transfers

Where Personal Data is transferred outside the EU/UK:

- SCCs will apply
- Supplementary measures (encryption, access controls) will be used
- Transfers will comply with Applicable Data Protection Laws

9. Audits and Inspections

9.1 Audit Rights

Controller may audit Processor's compliance:

- Once per year
- With 30 days' notice
- During normal business hours
- Without disrupting operations

9.2 Third-Party Audits

Processor may satisfy audit obligations by providing:

- SOC 2, ISO 27001, or similar certifications
- Penetration test summaries
- Security documentation

9.3 Confidentiality

Audit findings are confidential and may only be used for compliance purposes.

10. Data Subject Requests

Processor shall:

- Forward any Data Subject request to Controller
- Not respond directly unless instructed
- Assist Controller in fulfilling requests

11. Liability

Liability under this DPA is subject to the limitations set forth in the Principal Agreement, except where prohibited by law.

12. Termination

This DPA terminates automatically upon termination of the Principal Agreement.

Upon termination:

- Processor will delete or return Personal Data
- Backup deletion will follow standard retention cycles

13. Governing Law

This DPA is governed by the same law as the Principal Agreement.

14. Order of Precedence

If there is a conflict between this DPA and the Principal Agreement, this DPA prevails with respect to data protection matters.

ANNEX I — DETAILS OF PROCESSING

A. Nature and Purpose

Provision of a SaaS automation and workflow platform.

B. Categories of Data Subjects

As listed in Section 4.1.

C. Categories of Personal Data

As listed in Section 4.2.

D. Duration

For the duration of the Service.

ANNEX II — TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

Processor implements:

- Encryption (AES-256, TLS 1.3+)
- Access control and MFA
- Secure key management
- Network isolation

- Firewalls and IDS
- Logging and monitoring
- Regular vulnerability scanning
- Secure development lifecycle (SDLC)
- Encrypted in-memory sandbox environments
- Backup encryption and rotation
- Incident response procedures

ANNEX III — SUB-PROCESSORS

Name	Purpose	Location	Safeguards
OVH	Hosting	EU/Canada	SCCs, encryption
Wasabi	Storage	USA/EU	SCCs, encryption
Stripe	Payments	Global	Independent controller