Data Processing Addendum (DPA)

Effective Date: 2025-11-01
Last Updated: 2025-11-03

This Data Processing Addendum (“**DPA**”) forms part of the agreement between **NUBONS TECH LLC**, a WA LIMITED LIABILITY COMPANY, UBI Number: 605 973 469, with its principal place of business in **3818 186th SE, BOTHELL, WA, USA** ("NUBONS" or "Processor"), and the entity or organization that has accepted the NNP Terms of Use or an Order Form referencing them ("Customer" or "Controller"). This DPA reflects the parties’ agreement regarding the processing of Personal Data in connection with Customer’s use of NNP’s Platform-as-a-Service offerings (the "**Services**").

If there is any conflict between this DPA and the Agreement, this DPA controls the extent of the conflict with respect to the Processing of Personal Data.

1. Definitions

- **Agreement** means the master terms (e.g., Terms of Use), order forms, statements of work, and applicable policies governing Customer’s use of the Services.
- **Applicable Data Protection Laws** means data protection and privacy laws worldwide, including but not limited to: EU/EEA GDPR; UK GDPR and Data Protection Act 2018; Swiss FADP; CCPA/CPRA; Canada PIPEDA; Brazil LGPD; India DPDP Act 2023; Australia Privacy Act; and any implementing regulations.
- **Customer Personal Data** means Personal Data for which Customer is Controller and that NNP Processes on behalf of Customer as Processor in providing the Services.
- **Data Subject**, **Personal Data**, **Processing**, **Controller**, **Processor**, **Supervisor/Supervisory Authority** have the meanings set out in Applicable Data Protection Laws.
- **Security Incident** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by NNP.
- **Sub Processor** means any third party engaged by NNP that Processes Customer Personal Data on behalf of Customer.
- **Service Data** means telemetry, diagnostics, and operational data NNP processes as an independent controller to operate and secure the Services, as described in the Privacy Policy.

2. Roles, Processing Instructions

2.1 **Roles.** For Customer Personal Data, Customer is the Controller and NNP is the Processor.

2.2 **Instructions.** NNP will Process Customer Personal Data only (a) to provide and improve the Services; (b) as documented in the Agreement and this DPA; and (c) on Customer’s written instructions, including via configuration and use of the Services.

2.3 **Prohibited Data.** Customers will not submit special categories of data or other regulated data (e.g., PHI under HIPAA, PCI cardholder data, export-controlled technical data) unless the parties have executed the relevant addendum and enabled the corresponding program.

3. Confidentiality

NNP ensures that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations and receive privacy and security training.

4. Security

4.1 **Program.** NNP maintains an information security program aligned to industry standards (e.g., SOC 2/ISO 27001) and appropriate to the risks of Processing Customer Personal Data.

4.2 **Measures.** Without limitation, NNP implements the technical and organizational measures described in **Annex II** (including access controls, encryption in transit and at rest, key management, logging/monitoring, vulnerability management, secure development and change management, business continuity/disaster recovery, and incident response).

4.3 **Customer Responsibilities.** Customer is responsible for securing its configurations, credentials, identities, networks, and Customer-managed components (shared responsibility model), and for implementing appropriate access policies, backups, and multi-factor authentication.

5. Security Incidents

NNP will notify Customer without undue delay and in any event within **72 hours** after becoming aware of a Security Incident affecting Customer Personal Data. NNP will provide information reasonably available for Customer to meet its notification obligations, and will take reasonable steps to contain, investigate, and remediate the incident. Notifications will be sent to the Customer's designated contact(s).

6. Sub processors

6.1 **Authorization.** Customer authorizes NNP to engage Sub processors to Process Customer Personal Data.

6.2 **Contractual Requirements.** NNP will impose on Sub processors data protection obligations no less protective than those in this DPA and remains responsible for their performance.

6.3 **Changes.** NNP will provide advance notice of new Sub processors and allow Customer to object on reasonable, documented grounds relating to data protection. If the parties cannot resolve the objection, Customer may terminate the affected Services for convenience with a pro-rated refund of prepaid, unused fees.

7. Data Subject Requests

Considering the nature of Processing, NNP will provide reasonable assistance to Customer to respond to requests from Data Subjects to exercise their rights (access, rectification, deletion, restriction, portability, objection). Where a request is made directly to NNP, NNP will promptly forward it to Customer unless prohibited by law.

8. Impact Assessments and Consultation

NNP will provide Customer with reasonable cooperation and information to support data protection impact assessments and prior consultations with Supervisory Authorities, in each case solely as required by Applicable Data Protection Laws and considering the nature of the Processing and the information available to NNP.

9. Audits and Certifications

9.1 **Reports.** NNP will provide audit reports and certifications relevant to the Services (e.g., SOC 2 Type II, ISO 27001/27701 where applicable) and responses to reasonable security questionnaires.

9.2 **On-Site Audit.** Where required by Applicable Data Protection Laws and after exhausting the materials in Section 9.1, Customer may conduct an on-site audit up to once per year upon 30 days' notice, during business hours, subject to reasonable confidentiality, safety, and non-interference requirements. Customer will limit scope to systems and facilities used to Process Customer Personal Data and will reimburse NNP's reasonable costs.

10. International Data Transfers

10.1 **General.** NNP may Process and store Customer Personal Data in any country where NNP or its Sub processors operate, subject to this Section and the transfer mechanisms below.

10.2 **EEA/UK/Switzerland Transfers.** For restricted transfers: (a) the **EU Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914) apply as set out in **Annex I** and **Annex II** (Modules 2 and/or 3, as applicable); (b) the **UK International Data Transfer Addendum** (IDTA/Addendum) applies to UK transfers; and (c) the **Swiss Addendum** applies to Swiss transfers under the FADP.

10.3 **Supplementary Measures.** NNP implements technical and organizational measures to protect Customer Personal Data against access by public authorities that goes beyond what is necessary and proportionate in a democratic society, including encryption and access controls, as described in Annex II.

10.4 **Government Requests.** Where legally permitted, NNP will (i) notify Customer of government requests for Customer Personal Data; (ii) challenge unlawful or overbroad requests; and (iii) disclose only the minimum required to comply with a valid and binding order.

11. Return and Deletion

Upon termination or expiry of the Agreement, NNP will, upon Customer request, return Customer Personal Data in a commonly used format and then delete or anonymize such data within **30 days**, unless retention is required by law or to establish, exercise, or defend legal claims.

12. Liability

Liability under this DPA is subject to the limitations of liability in the Agreement. Nothing in this DPA limits the rights of Data Subjects under Applicable Data Protection Laws.

13. CCPA/CPRA - Service Provider Terms

To the extent NNP Processes Personal Information of California residents on behalf of Customer, NNP acts as a **Service Provider** and will: (a) Process the Personal Information only for the business purposes described in the Agreement and this DPA; (b) not **sell** or **share** the Personal Information; (c) not combine Personal Information received from Customer with Personal Information from other sources except as permitted by CPRA; (d) assist Customer in responding to consumer requests; and (e) enable audits as required by CPRA. Customer will provide the required notices and obtain required consents.

14. India (DPDP Act 2023)

Where the DPDP Act applies, NNP acts as a **Data Processor** and will Process Personal Data per Customer's instructions; implement reasonable security safeguards; notify Customer and the Board of a Personal Data breach where required; and assist Customer in fulfilling data principal rights requests. Customer appoints NNP as its authorized Data Processor and confirms lawful grounds for Processing.

15. Updates

NNP may update this DPA where required to comply with law or to reflect new transfer mechanisms. Material adverse changes will take effect 30 days after notice unless required sooner by law.

16. Contact

NNP Privacy: contact@nubons.com
Security: contact@nusbons.com
NUBONS TECH LLC

UBI Number: 605 973 469
3818 186th SE, BOTHELL, WA, USA

Annex I — Description of Processing and SCC Details

A. Parties

- **Data Exporter (Controller):** Customer (details per Order).
- **Data Importer (Processor):** NUBONS TECH LLC, UBI Number: 605 973 469, 3818 186th SE, BOTHELL, WA, USA, Contact: contact@nubons.com.

B. Description of Transfer

- **Categories of Data Subjects:** Customer's users, employees/contractors, end customers, and other individuals whose data is included in Customer Content.
- **Categories of Personal Data:** Common identifiers (name, email, IP), account metadata, usage/telemetry, content uploaded or generated by Customer or its end users. Customer may include special categories only if expressly agreed in writing and configured for the relevant regulated-data program.
- **Sensitive Data:** Not intended to be processed unless the parties execute the applicable addendum and enable controls.
- **Frequency of Transfer:** Continuous for the duration of the Agreement.
- **Subject Matter and Nature of Processing:** Hosting, storage, transmission, computation, logging/monitoring, support, and security operations necessary to provide the Services.
- **Purpose(s) of Processing:** Provision, maintenance, and improvement of the Services; security; support; billing; compliance with law.
- **Duration:** For the term of the Agreement plus the return/deletion period in Section 11.
- **Competent Supervisory Authority (EEA):** Determined under Clause 13 of the SCCs based on the exporter's location.

C. SCC Modules and Options

- **Module 2 (Controller→Processor):** Applies where Customer is Controller and NNP is Processor.
- **Module 3 (Processor→Processor):** Applies where Customer acts as a Processor for its own clients and engages NNP as a sub-processor (Customer warrants it has authority to execute the SCCs on behalf of the Controller).
- **Docking Clause (Clause 7):** Enabled.
- **Clause 9(a) — Use of Subprocessors:** Option 2 (general authorization) with advance notice via the Subprocessor page.
- **Clause 11(a) — Redress:** Not applicable.
- **Clause 17 — Governing Law:** Laws of **Ireland** (for EEA transfers).
- **Clause 18 — Forum and Jurisdiction:** Courts of **Ireland** (for EEA transfers).

D. UK Addendum

The UK Addendum (A3, version per ICO) is incorporated; the competent authority is the ICO; the governing law and forum are England and Wales. Information for Tables 1–4 is populated by Annex I and Annex II.

E. Swiss Addendum

For Swiss FADP transfers, references to the GDPR in the SCCs are deemed references to the FADP; the competent authority is the FDPIC; governing law and forum are Switzerland; “sensitive data” is interpreted per FADP.

Annex II — Technical and Organizational Measures (TOMs)

1. **Governance & Policies**: Documented information security program; executive oversight; risk management; security awareness and role-based training; vendor risk management.
2. **Access Control & Identity**: Least privilege; role-based access; SSO/MFA for admins; just-in-time access; periodic access reviews; logical segregation by tenant.
3. **Encryption & Key Management**: TLS 1.2+ in transit; AES-256 at rest; managed KMS; key rotation; options for customer-managed keys (CMK) where available.
4. **Network Security**: Segmented VPC/VNet; firewalls/security groups; WAF; DDoS protections; private connectivity options; vulnerability scanning.
5. **Application Security**: Secure SDLC; code reviews; dependency scanning/SCA; SAST/DAST; secrets management; change management with approvals.
6. **Logging & Monitoring**: Centralized logging; tamper-resistant logs; SIEM; anomaly detection; audit trails retained per plan; time synchronization.
7. **Endpoint & Platform Security**: Hardening baselines; EDR; patch management; container runtime security; image signing and scanning; supply-chain controls.
8. **Data Management**: Backups; replication; tested restore; data minimization; deletion workflows; data classification and handling standards.
9. **Business Continuity & DR**: Documented BCP/DR; RTO/RPO targets per service tier; periodic tests; capacity management.
10. **Incident Response**: 24×7 monitoring; playbooks; forensics; customer comms templates; lessons-learned and corrective actions.
11. **Physical & Environmental**: Tier-appropriate data centers; access badges/biometrics; CCTV; visitor logging; power/cooling redundancy; fire detection/suppression.
12. **Personnel**: Background checks per law; confidentiality agreements; termination/role change off-boarding; least-privilege workstation access.
13. **Privacy by Design**: DPIA templates; pseudonymization; data masking; minimization; secure defaults; feature reviews for privacy impact.
14. **Certification & Testing**: External audits (e.g., SOC 2/ISO 27001); independent penetration tests at least annually; remediation tracking.

Annex III — Sub processors (Illustrative; to be customized)

- Cloud infrastructure providers (IaaS) in regions where Services operate.
- Managed database, logging, and monitoring vendors.
- Support tooling and ticketing systems.
- Email/SMS communication providers.
- Payment processors for billing and collections.

Annex IV — Data Processing Details for CCPA/CPRA

- **Business Purpose(s):** Providing PaaS services, ensuring security, debugging, auditing interactions, short-term transient use, internal R&D to improve service quality.
- **Categories of Personal Information:** Identifiers; internet/network activity; geolocation (coarse, IP-based); professional information; inferences limited to service operations; sensitive personal information not sought or used for inferring characteristics.