Orca1 Data Processing Addendum (DPA)

Last Updated: January 28, 2026

This Data Processing Addendum (“**DPA**”) forms part of the agreement between Orca1 (“**Orca1**”, “**Processor**”, “**Service Provider**”) and the customer (“**Customer**”, “**Controller**”, “**Business**”) governing Customer’s use of the Orca1 services (“**Agreement**”).

This DPA applies where Orca1 processes Personal Data on behalf of Customer in connection with the Services and reflects the parties’ obligations under applicable data protection laws, including the EU General Data Protection Regulation (“**GDPR**”), UK GDPR, and applicable U.S. state privacy laws (including CCPA/CPRA).

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

---

1. Definitions

Capitalized terms not defined here have the meanings set forth in the Agreement or applicable data protection law.

- **Customer Data:** Any data, including Personal Data, submitted to the Services by or on behalf of Customer.
- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Processing:** Any operation performed on Personal Data, including collection, storage, use, disclosure, or deletion.
- **Subprocessor:** Any third party authorized by Orca1 to process Personal Data on behalf of Customer.
- **Security Incident:** A confirmed breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

---

2. Roles and Scope of Processing

2.1 Roles

Customer is the Controller (or Business) of Customer Data. Orca1 acts solely as a Processor (or Service Provider) on Customer’s behalf.

2.2 Purpose Limitation

Orca1 shall process Customer Data **solely** to provide, maintain, secure, and support the Services in accordance with the Agreement and Customer's documented instructions.

2.3 Customer Responsibility

Customer is solely responsible for: (a) determining the legality of Processing; (b) obtaining all required notices and consents; (c) ensuring Customer Data complies with applicable law; and (d) configuring the Services appropriately.

2.4 No Ownership Transfer

Customer retains all ownership rights in Customer Data. Orca1 acquires no ownership interest in Customer Data.

---

3. No AI / Model Training

Orca1 **does not use Customer Data or end-user content to train machine learning models, artificial intelligence systems, or foundation models**, unless expressly authorized in writing by Customer.

This restriction applies to both internal and external models and survives termination of the Agreement.

---

4. Confidentiality

Orca1 shall ensure that any person authorized to process Customer Data is bound by confidentiality obligations no less protective than those in this DPA and receives appropriate data protection training.

---

5. Security Measures

5.1 Safeguards

Orca1 shall implement appropriate administrative, technical, and organizational measures designed to protect Customer Data against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Such measures include, without limitation:

- Encryption in transit (TLS) and at rest where appropriate;
- Access controls and role-based authorization;
- Secure development practices and vulnerability management;
- Network segmentation and monitoring;
- Incident detection and response procedures.

5.2 Security Certifications

Orca1 maintains a security program aligned with recognized standards such as SOC 2 Type II and ISO 27001 (where applicable).

---

6. Subprocessing

6.1 Authorization

Customer grants Orca1 general authorization to engage Subprocessors to process Customer Data.

6.2 Obligations

Orca1 shall impose data protection obligations on Subprocessors that are no less protective than those in this DPA.

6.3 Transparency

A current list of Subprocessors and their functions shall be made available upon request or via Orca1’s website.

6.4 Objection Right

Customer may object to a new Subprocessor on reasonable data protection grounds within ten (10) business days of notice. If the objection cannot be resolved, Customer may terminate the affected Services without penalty.

6.5 Liability

Orca1 remains responsible for Subprocessor compliance with this DPA.

---

7. International Data Transfers

7.1 Transfer Mechanisms

Where Customer Data is transferred outside the EEA, UK, or Switzerland, Orca1 shall implement appropriate safeguards, including:

- European Commission Standard Contractual Clauses (“SCCs”);
- UK Addendum to SCCs;
- Adequacy decisions or other lawful transfer mechanisms.

7.2 SCC Incorporation

Where applicable, the SCCs (Controller-to-Processor, Module Two) are incorporated by reference and form part of this DPA.

7.3 Government Access Requests

Orca1 will challenge unlawful or overbroad government requests for Customer Data and notify Customer unless legally prohibited.

---

8. Data Subject Requests

8.1 Customer Responsibility

Customer is responsible for responding to Data Subject Requests.

8.2 Assistance

Orca1 shall provide reasonable assistance to Customer to fulfill such requests, including access, correction, deletion, restriction, portability, or objection requests, to the extent technically feasible and legally required.

8.3 Direct Requests

If Orca1 receives a request directly from a data subject relating to Customer Data, Orca1 shall notify Customer unless legally prohibited.

---

9. Security Incident Response

9.1 Notification

Orca1 shall notify Customer without undue delay and, where feasible, within seventy-two (72) hours after becoming aware of a Security Incident affecting Customer Data.

9.2 Information Sharing

Orca1 shall provide reasonable information about the nature of the incident, affected data categories, mitigation steps, and corrective actions.

9.3 Cooperation

Orca1 shall cooperate with Customer in fulfilling any breach notification obligations to regulators or data subjects.

---

10. Deletion and Return of Data

Upon termination or expiration of the Agreement, Orca1 shall delete or return Customer Data within the timeframe specified in the Agreement or applicable DPA, unless retention is required by law. Upon request, Orca1 shall certify deletion.

---

11. Audits and Compliance

11.1 Audit Rights

Customer may audit Orca1's compliance with this DPA through reasonable written requests, third-party certifications (e.g., SOC 2 reports), or mutually agreed assessments, subject to reasonable confidentiality and security restrictions.

11.2 Cooperation

Orca1 shall provide reasonable cooperation to demonstrate compliance with this DPA.

---

12. Assistance with DPIAs and Regulatory Inquiries

Orca1 shall provide reasonable assistance with:

- Data protection impact assessments (DPIAs);
- Prior consultations with supervisory authorities;
- Regulatory inquiries related to Processing under this DPA.

---

13. CCPA / CPRA Terms (U.S.)

Where Orca1 processes Personal Information subject to the CCPA/CPRA:

- Orca1 acts as a **Service Provider** and **Contractor**.
- Orca1 shall not sell or share Personal Information.
- Orca1 shall not retain, use, or disclose Personal Information outside the business purposes defined in the Agreement.
- Orca1 shall comply with applicable verification and assistance obligations.

---

14. Confidential Business Information

Customer Data constitutes Customer's confidential business information. Orca1 shall protect Customer Data accordingly and restrict access on a need-to-know basis.

---

15. Liability and Remedies

Except as required by applicable law, Orca1's liability arising from or related to this DPA shall be subject to the limitations of liability set forth in the Agreement.

---

16. Order of Precedence

In the event of conflict between this DPA and the Agreement, this DPA controls with respect to data protection matters.

---

17. Term and Survival

This DPA remains in effect for the duration of Orca1's Processing of Customer Data and survives termination of the Agreement until all Customer Data has been deleted or returned.

---

18. Annex A — Details of Processing

A.1 Subject Matter

Provision of Orca1's SaaS platform and related services.

A.2 Duration

For the term of the Agreement and any legally required retention period.

A.3 Nature and Purpose of Processing

Hosting, storage, transmission, retrieval, analysis, support, security, and maintenance of Customer Data as necessary to provide the Services.

A.4 Categories of Data Subjects

Customer’s employees, contractors, agents, business contacts, end users, and other individuals whose data is submitted to the Services.

A.5 Categories of Personal Data

Business contact information, professional identifiers, usage data, communications, regulatory records, and other data submitted by Customer.

A.6 Special Categories of Data

None intentionally; Customer agrees not to upload special categories unless expressly authorized and legally permitted.

---

19. Annex B — Technical and Organizational Measures

Orca1 maintains a comprehensive information security program, including:

- Encryption in transit and at rest where appropriate;
- Role-based access control and least privilege enforcement;
- Continuous monitoring and intrusion detection;
- Secure software development lifecycle (SDLC);
- Regular vulnerability assessments and penetration testing;
- Incident response and disaster recovery procedures;
- Employee security training and confidentiality obligations;
- Vendor risk management and due diligence.