Orca1 Privacy Policy

Last updated: January 28, 2026

Privacy at a Glance

We collect only the data necessary to operate and improve Orca1.

Customer-uploaded data belongs to our customers — we do not sell it or use it to train AI models.

We use industry-standard security controls to protect data.

You can access, correct, or delete your personal data.

Orca1 does not sell personal data or use it for consumer advertising.

Orca1 (“**Orca1**”, “**we**”, “**us**”, or “**our**”) operates the Orca1 platform and related websites and services (the “**Service**”). This Privacy Policy explains what personal data we collect, why we collect it, how we use and share it, and the rights available to you with respect to your personal data.

If you are an Orca1 customer (an entity that has a commercial agreement with Orca1) or an end-user of a customer (e.g., your employer uses Orca1), the commercial agreement and any executed Data Processing Addendum (DPA) between Orca1 and your employer govern the processing of Customer Data. This Privacy Policy describes how we handle personal data that we collect directly and information we process as a service provider.

If anything in this policy conflicts with a signed DPA or contract, the terms of that DPA/contract will prevail for the data covered by it.

---

1. Scope and Applicability

This Policy applies to personal data collected by Orca1 through:

- our websites (e.g., https://orca1.ai/) and documentation portals;
- our SaaS platform and APIs;
- marketing and sales processes (forms, events, newsletters);
- support, professional services, and communications.

It does **not** govern the privacy practices of third parties that Orca1 does not control (e.g., social networks, payment processors, cloud providers) except as described below.

---

2. Definitions

- **Personal data / personal information:** any information that identifies or can reasonably identify an individual.
- **Customer Data:** any data, including personal data, submitted to the Service by or on behalf of a customer. Orca1 processes Customer Data solely on the customer's instructions and does not determine the purposes or means of such processing. Customers remain the data controller (or equivalent legal role) for Customer Data, and Orca1 acts as a processor or service provider. Orca1 is not responsible for the legality, accuracy, or content of Customer Data.
- **Service Data (or System Data):** technical or usage data collected by Orca1 in operating, improving, and securing the Service (e.g., logs, telemetry).
- **Sensitive personal data:** data revealing race, religion, health, or similar highly sensitive categories (we treat these with additional safeguards and will only process when expressly permitted).

---

3. Categories of Data We Collect

A. Account & Identity Data

- Contact name, email address, phone number, job title, organization, billing name and address.
- Login credentials (hashed and salted), authentication tokens, multi-factor authentication data.

B. Customer Data (provided to Orca1 by customers)

- Documents, records, and datasets uploaded by customers (may include names, business contact details, descriptions of individuals, regulatory filings, investigator/establishment profiles).
- Search queries, annotations, saved reports, workspace content.

Note: Customer Data is processed under customers' instructions. Orca1 is not responsible for

the legality, accuracy, or content of Customer Data that customers they upload.

C. Payment & Billing Data

- Payment method details (processed by our payment processors), billing contact information, invoices, purchase history.

D. Usage, Device & Technical Data

- IP address, device type, browser, operating system, time stamps, pages visited, feature usage, error logs, performance metrics, API usage metrics.

E. Communications Data

- Emails, chat messages, support tickets, recordings you send to or receive from Orca1.

F. Cookies and Similar Technologies

- Session cookies, persistent cookies, local storage for remembering preferences, and tracking pixels. See Section 9 (Cookies).

G. Analytics & Third-party Data

- Aggregated and anonymized usage statistics; information from third-party sources (e.g., public regulatory databases) that we integrate into the Service.

---

4. How We Use Personal Data (Purposes)

We process personal data for legitimate business purposes including:

1. **Provisioning and operating the Service:** authenticate users, provide access, maintain accounts, deliver platform features, support APIs.
2. **Customer support & professional services:** respond to requests, troubleshoot, and provide training or onboarding.
3. **Billing and payments:** invoice customers, process payments, detect and prevent fraud.
4. **Security, reliability & abuse prevention:** detect incidents, prevent unauthorized access, diagnose problems, and protect our systems.
5. **Product improvement & research:** analyze usage to improve features, fix bugs, and plan roadmaps (generally on pseudonymized / aggregated data).
6. **Legal and regulatory compliance:** comply with legal obligations, enforce terms, respond to

lawful requests.
7. **Marketing and commercial operations:** send product announcements, newsletters, event invites, and tailor marketing (where permitted); you can opt out (see Section 11).
8. **Third-party integrations:** enable customer-authorized integrations with approved third parties.

No AI / Model Training. Orca1 does not use Customer Data or end-user content to train machine learning or artificial intelligence models unless expressly authorized in writing by the customer.

If we need to process data for a purpose other than those listed here, we will notify you and obtain any required consent.

---

5. Legal Bases for Processing (GDPR)

Where the GDPR applies, our legal bases for processing personal data include:

- **Performance of a contract:** to provide the Service and fulfill contractual obligations.
- **Legal compliance:** to comply with applicable laws and regulatory obligations.
- **Legitimate interests:** for system security, fraud prevention, product improvement, and direct marketing to business contacts (balanced against individual rights).
- **Consent:** where required (e.g., some marketing cookies or non-essential tracking).

---

6. How We Share and Disclose Data

We may share personal data as follows:

- **With service providers / subprocessors.** We use third-party vendors to provide hosting, analytics, customer support, payment processing, email delivery, and other services. These vendors act as processors and are bound by contractual obligations to safeguard data.
- **With customers.** Customer Data is accessible to authorized users within the customer's organization and to those the customer authorizes.
- **With affiliates.** Orca1 affiliates may access data to support operations (subject to this Policy).
- **For legal reasons.** To respond to valid legal processes, investigations, governmental requests, and to enforce our agreements.
- **Business transfers.** In the event of a merger, acquisition, sale, or bankruptcy, personal data may be transferred as part of the transaction (we will notify affected users where required).
- **Aggregated / anonymized data.** We may share or publish de-identified and aggregated information that does not reasonably identify individuals.
- **Government requests.** We may disclose data where legally required. Where permitted by law, we will notify affected customers before disclosure and challenge requests we believe are unlawful or overly broad.

Before granting a vendor access to Customer Data, we conduct due diligence and require contractual commitments (including data security, confidentiality, and restrictions on onward transfers). A list of major subprocessors and their purposes is available upon request.

---

7. International Transfers

Orca1 may transfer personal data to countries outside your jurisdiction, including the United States. When we transfer personal data internationally, we use appropriate safeguards (e.g., standard contractual clauses, reliance on adequacy decisions, or other lawful mechanisms) where required by law.

---

8. Data Retention

We retain personal data only as long as necessary for the purposes listed in this Policy, to satisfy contractual obligations, to comply with legal obligations, resolve disputes, and enforce agreements.

Typical retention practices include:

- Account and billing data: retained while the account is active and for a commercially reasonable period (e.g., up to 7 years) thereafter for accounting and legal compliance.
- Support and communications: retained for the duration necessary to resolve issues, typically 2–7 years.
- Logs/technical data: retention period balanced for security and debugging needs (may be short — e.g., 30–90 days — or longer for aggregated logs).

Upon termination of a customer account, Orca1 will delete or return Customer Data within the timeframe specified in the applicable customer agreement or DPA, unless retention is required by law.

Retention periods vary by data type and legal requirements. If you need a specific retention schedule for your Customer Data, contact us or refer to your DPA.

---

9. Cookies & Tracking Technologies

We use cookies and similar technologies to operate the Service, analyze usage, and support marketing. Categories:

- **Essential cookies:** required for platform login and security.
- **Performance/analytics cookies:** measure usage and performance.
- **Functional cookies:** remember preferences and settings.
- **Advertising/tracking cookies:** used for marketing where permitted.

You can manage cookie preferences through your browser and, where provided, our cookie controls. Blocking cookies may affect Service functionality.

---

10. Security

Orca1 treats Customer Data as confidential business information and implements administrative, technical, and organizational safeguards designed to protect it against unauthorized access, disclosure, alteration, or destruction.

Examples include:

- Access controls and encryption in transit (TLS) and at rest where appropriate;
- Network security controls and firewalls;
- Regular vulnerability scanning, patch management, and secure development practices;
- Employee training and limited access on a “need-to-know” basis.

No system is perfectly secure; we continually evaluate and improve our controls. In the event of a confirmed data breach affecting personal data, Orca1 will follow applicable breach-notification laws and inform affected parties and regulators as required.

Except as required by applicable law, Orca1’s obligations and liability related to security incidents are governed by the applicable customer agreement and DPA.

---

11. Your Privacy Rights

If you are located in the EU / EEA (GDPR)

You may have the right to:

- **Request access** to personal data we hold about you.
- **Request correction** of inaccurate data.
- **Request deletion** of personal data (“right to be forgotten”) in certain circumstances.
- **Request restriction** of processing.
- **Object** to processing where we rely on legitimate interests.
- **Data portability**: obtain a copy of your personal data in a structured, machine-readable format.

To exercise these rights, contact us (see Section 15). We aim to respond to verified requests within 30 days (or sooner where required by law). Requests are generally free of charge unless they are manifestly unfounded or excessive.

Requests from data subjects acting on behalf of an organization may be directed to that organization (customer) if we are processing data under their instructions.

If you are located in California (CCPA / CPRA)

Subject to eligibility, California residents have rights including:

- **Right to know** categories of personal information collected, disclosed, or sold and the purpose.
- **Right to access**: request specific pieces of personal information.
- **Right to delete**: request deletion of personal information.
- **Right to opt-out** of sale or sharing for targeted advertising (Orca1 does not sell personal information for consumer marketing purposes; customer data is processed under contract).
- **Non-discrimination** for exercising rights.

Submit CCPA/CPRA requests via the contact methods in Section 15. We will verify requests to the extent required by law.

Authentication & Authorized Requests

To protect privacy, we may need to verify identity and authority before fulfilling requests. Where your request concerns Customer Data processed on behalf of a business, we generally direct you to the customer (the data controller) so they can make requests regarding that data.

---

12. Children

The Service is not directed to children under 16. We do not knowingly collect personal data from children under 16. If you believe we have collected personal data from a child under 16, contact us to request deletion.

13. Third-Party Links & Embedded Content

Our websites and Services may include links or embedded content from third parties (e.g., regulatory databases, social widgets). We are not responsible for third-party privacy practices. Review their privacy policies before providing personal data.

---

14. Data Processing Addendum (DPA)

For customers in jurisdictions that require a DPA (e.g., GDPR), Orca1 offers a DPA that defines roles, security obligations, subprocessors, international transfer mechanisms, and assistance with data subject requests. Customers may request a copy via the contact details in Section 15.

---

15. Data Ownership and Control

Customer Data remains the property of the applicable customer. Orca1 acquires no ownership rights in Customer Data and processes such data solely to provide and improve the Service in accordance with customer instructions and applicable law.

---

16. No Sale or Commercialization of Personal Data

Orca1 does not sell personal data, rent personal data, or disclose personal data for cross-context behavioral advertising purposes. Customer Data is never monetized.

---

17. Data Location

Orca1 operates a globally distributed infrastructure. Unless otherwise agreed in writing, we do not guarantee that personal data will be stored or processed in a specific geographic location.

18. Contact & Privacy Requests

To exercise rights, request a DPA, inquire about subprocessors, request a copy of Orca1's standard contractual clauses, or report privacy concerns:

- Email: contact@orca1di.com
- Mailing address: Orca1, 56 Newton Rd, Woodbridge, CT 06525
- For data protection authority complaints (EU): you may contact your local supervisory authority.

---

19. Changes to this Privacy Policy

We may update this Privacy Policy to reflect legal, technical, or business changes. When we do, we will revise the "Last updated" date and, where required by law or the significance of the change, provide additional notice (e.g., email, in-product notice).

---

20. Additional Practical Notes for Orca1 Customers

- **Data minimization:** advise customers to minimize sensitive personal data uploaded to Orca1 wherever feasible; provide configuration options to mask or pseudonymize sensitive fields.
- **Access controls / SSO:** encourage customers to use SSO and strong authentication; Orca1 supports role-based access controls.
- **Audit logging:** Orca1 retains audit logs for security and compliance — include log retention schedule in your DPA.
- **Subprocessor transparency:** maintain and publish an up-to-date list of subprocessors and the categories of data they process.
- **Breach playbook:** implement an incident response plan that includes notification timelines consistent with relevant laws (e.g., 72 hours for GDPR where applicable).

---

21. Example Subprocessors

- DNS: CloudFlare
- Payment processing: Stripe
- Email delivery: SendGrid
- Identity and SSO: Google, LinkedIn

22. Acknowledgement

By using Orca1, you acknowledge that you have read and understood this Privacy Policy and that you consent to our processing of personal data as described herein (to the extent consent is the lawful basis).