Orb Labs AG — Privacy Policy

Orb Labs AG — Privacy Policy Last updated: June 22nd, 2026 · Version 1.0

---

1. Who is responsible (controller)

Orb Labs AG (UID: **CHE-340.555.145**), Untere Roostmatt 8 6300, Zug, Switzerland, is the controller for the processing described here.

2. Scope

This Policy explains how we process personal data when you visit our website, when you engage us or interact with us as a client or business contact, when we contact you as a prospective client, and when individuals are referenced in our research.

3. Whose data we process, and what we collect

We process personal data about four groups:

a) Website visitors. Technical data (IP address, device/browser, pages viewed, referrer), and any data you submit through forms or by contacting us. Sources: you, and cookies/analytics (Section 6).

b) Clients and business contacts. Name, business contact details, role/organization, correspondence, engagement and scope records, NDA records, and billing/payment information. Sources: you, your organization, and our payment processor.

c) Prospective clients (outbound outreach). Business contact and professional-profile information (e.g., name, role, employer, professional social-media profile data) used to identify and contact potential institutional clients. Sources: public professional sources and profiles, business networks, and third-party lead/enrichment tools.

d) Individuals referenced in research (evaluated third parties). When a report assesses a target company, it may include professional information about its founders and core team — e.g., professional background, track record, publicly visible code-repository or governance activity, and, where relevant, on-chain activity associated with a public identifier. Sources: information provided by the client (data room) and publicly available information. We assess such individuals in their professional/business capacity only.

We do not intentionally collect special-category / sensitive data, and we do not direct our services to children.

4. Why we process data, and on what basis

Purpose	**Data groups**	**Basis (GDPR terms; FADP applies in parallel)**
Operate and secure the website	a	Legitimate interest
Respond to enquiries; manage the relationship	a, b	Pre-contract steps / legitimate interest
Deliver engagements; produce reports	b, d	Contract performance; legitimate interest (research)
Billing, accounting, records	b	Legal obligation; contract
Identify and contact prospective clients	c	Legitimate interest (B2B outreach) — subject to opt-out
Confidentiality, NDA and compliance records	b	Legal obligation; legitimate interest
Analytics / service improvement	a	Consent (where required) / legitimate interest

Under the revised FADP, processing must in all cases be lawful, proportionate, transparent, and conducted in good faith. Where we rely on legitimate interest, we balance it against the rights of the data subjects concerned.

5. Research on third parties — additional note

Reports assess individuals only in their professional capacity, present good-faith professional opinion rather than statements of fact, and are confidential to the named client (not published). Data subjects in this group retain the rights in Section 11; given the confidential and time-limited nature of the work, certain rights may be subject to lawful restrictions [confirm with counsel].

6. Cookies and analytics

We use [necessary cookies / analytics: name, e.g., Plausible/GA4]. Where consent is required, we request it via our cookie banner, set to decline non-essential cookies by default. You can manage preferences at [link]. [List specific tools and their providers.]

7. Who we share data with (processors and recipients)

We share data only as needed with: hosting/website provider, analytics provider, email/communication provider, payment processor, lead/enrichment tool(s) , and our newsletter provider Substack (if you subscribe). We require processors to protect data under written agreements. We do not sell personal data. We may disclose data where legally required.

8. International transfers

Some providers are located outside Switzerland/the EEA (e.g., in the United States). Where we transfer personal data abroad, we rely on an adequate-protection determination or appropriate safeguards (e.g., Standard Contractual Clauses with any necessary supplementary measures).

9. Retention

We keep personal data only as long as necessary for the purposes above or as required by law (e.g., Swiss bookkeeping retention for accounting records [~10 years]).

10. Security

We apply technical and organizational measures appropriate to the risk, including access controls, encryption in transit, confidentiality obligations, and controlled handling of client data-room materials. No method of transmission or storage is completely secure.

11. Your rights

Subject to applicable law, you may request access to, and rectification or deletion of, your personal data; restriction of or objection to processing; and data portability; and you may withdraw consent at any time. You may lodge a complaint with the Swiss Federal Data Protection and Information Commissioner (FDPIC), and — if the GDPR applies to you — with your local supervisory authority.

12. Automated decision-making and profiling

We do not make decisions producing legal or similarly significant effects on individuals solely by automated means. Our research involves human professional judgment.

13. Changes

We may update this Policy; the current version is published here with its date.