Privacy Policy

Effective Date: June 1, 2026

This Privacy Policy explains how Optic, Inc., doing business as BIOPTIC ("**BIOPTIC**", "**we**", "**us**"), collects, uses, shares and protects information in connection with bioptic.io, the BIOPTIC platform, and our research and analysis engagements.

BIOPTIC provides an agentic AI platform for the pharmaceutical industry, available to organisations under paid licences and subscriptions, together with expert research and analysis engagements. For most website visitors, the only personal information we hold is a business email address. For platform users, we also maintain the account, subscription and usage records described below.

If your organisation has a separate written agreement with us — an enterprise agreement, order form, statement of work or data processing agreement — **that agreement controls over this Policy** with respect to Customer Content, to the extent the two conflict.

---

1. Who we are

Optic, Inc. (d/b/a BIOPTIC) 535 Mission Street, San Francisco, CA 94105, United States
office@bioptic.io

For information collected through bioptic.io, and for account, subscription, billing and usage data, BIOPTIC is the controller. Where we process Customer Content on a customer's behalf — through the platform or under an engagement — we act as a processor on that customer's documented instructions, under a data processing agreement available on request.

[CONFIRM with counsel: if BIOPTIC actively offers services to organisations in the EU/UK without an establishment there, Article 27 GDPR may require appointing an EU and/or UK representative — if appointed, name them here.]

---

2. What we collect

2.1 Website visitors

If you contact us through bioptic.io — by submitting a project enquiry, requesting a sample report, or subscribing to updates — **we collect your business email address, and any name, organisation and message you choose to provide.**

We do not use advertising or third-party tracking cookies on bioptic.io. We use only cookies strictly necessary for the site to function, together with basic aggregate analytics that do not identify you individually. If we introduce non-essential cookies, we will ask for your consent first.

2.2 Clients and prospective clients

In the course of a commercial relationship we hold ordinary business contact information — name, business email, telephone number, job title and organisation — for the people we work with, along with correspondence, contract and billing records.

2.3 Accounts and subscriptions

When your organisation purchases a licence or subscription to the BIOPTIC platform, or is granted access as an authorised partner, we create accounts for its users. For each account we hold:

- name, business email, organisation and role;
- authentication data — single sign-on identifiers or credentials (passwords are stored only in hashed form);
- account settings and preferences;
- subscription records — plan, seats, entitlements, invoices and payment status.

Billing is normally by invoice. Where card payments are used, they are handled by a payment processor; we do not store full card numbers. *[CONFIRM current payment flow.]*

2.4 Usage and device data

When you use the platform or bioptic.io, we collect log and usage information: IP address, browser and device type, pages and features used, timestamps, and diagnostic and security events. We use this to operate, secure, support and improve the service — not to build advertising profiles.

2.5 Customer Content

"**Customer Content**" means the briefs, prompts, documents, datasets, instructions and other materials you or your users submit to the platform or provide to us for an engagement, together with the research outputs, source citations and deliverables produced from them.

Customer Content is handled as confidential. **We do not sell it, share it with other customers, or disclose it to third parties except as described in Section 5.**

The platform works primarily with publicly available and licensed commercial sources — registries, regulatory filings, patents, publications and similar. Customer Content is used only to provide the service to that customer.

We ask you not to upload patient-level personal data, identifiable health information, or other special-category personal data unless we have agreed to it in writing in advance and an appropriate data processing agreement is in place. Our services do not require personal data beyond business contact details.

---

3. Why we process information, and on what legal basis

Purpose	**Legal basis (UK/EU GDPR)**
Responding to enquiries and sending requested materials	Legitimate interests; consent where required
Creating and administering accounts, subscriptions and licences	Performance of a contract
Providing, securing, supporting and improving the platform	Performance of a contract; legitimate interests
Negotiating, entering into and performing engagements	Performance of a contract
Producing, reviewing and delivering research and analysis	Performance of a contract; legitimate interests
Quality assurance and internal evaluation of our own systems	Legitimate interests
Billing, accounting and record-keeping	Legal obligation; performance of a contract

Purpose	Legal basis (UK/EU GDPR)
Security, fraud prevention and enforcing our terms	Legitimate interests; legal obligation
Sending updates about our work, where you have asked for them	Consent; legitimate interests

Where we rely on legitimate interests, we have assessed that our interest in operating and improving a professional software and research business does not override your rights.

We do not make automated decisions about individuals that produce legal or similarly significant effects. Our AI systems research and analyse markets, companies and assets — not people.

You can withdraw consent, or unsubscribe from updates, at any time — every message includes an unsubscribe link, or you can write to office@bioptic.io.

---

4. AI models and training

We use our own agentic platform together with third-party foundation models from commercial providers to process and analyse information.

We do not use Customer Content — prompts, uploads, or outputs — to train, fine-tune or improve any model that serves any other customer.

Where Customer Content is processed by a third-party model provider as part of providing the service, we use enterprise or API arrangements that contractually prohibit the provider from using that content for model training, and we configure those services accordingly, including limited- or zero-retention settings where the provider offers them.

Our internal evaluation work uses our own work product and material that has been de-identified so that it contains no customer confidential information and cannot reasonably be attributed to a customer.

---

5. Who we share information with

We do not sell personal information, we do not share it for cross-context behavioural advertising, and we have not done either in the preceding twelve (12) months.

We share information only with:

- **Infrastructure and hosting providers.** Our systems run on Google Cloud Platform, in a secured, access-controlled environment.
- **Foundation model providers**, where processing is necessary to provide the service, under terms that prohibit training on that content (Section 4).
- **Business service providers** — for example, email, document storage, billing, payment processing and support tooling — acting on our instructions under written agreements.
- **Professional advisers**, such as legal and accounting advisers, under duties of confidentiality.
- **Authorities**, where we are legally required to disclose, or where necessary to establish, exercise or defend legal claims. Where a request concerns Customer Content, we will notify the affected customer before disclosing unless legally prohibited from doing so.
- **A successor entity**, in connection with a merger, acquisition or sale of assets, subject to this Policy continuing to apply.

A current list of the sub-processors we use to handle Customer Content is available on request at **office@bioptic.io**. Where a data processing agreement is in place, it provides advance notice of new sub-processors and a right to object on reasonable data protection grounds.

We do not disclose Customer Content to any other customer, and we do not identify a customer publicly without their written consent.

---

6. Who can access customer data internally

Access to Customer Content is limited to **authorised BIOPTIC personnel who need it to provide or support the service** — the delivery team assigned to an engagement, the experts who review output before it ships, support staff assisting a user at their request, and a small number of engineering and security staff maintaining the systems.

Access is role-based, individually authenticated, logged, and reviewed on a regular schedule. Everyone with access is bound by written confidentiality obligations, and personnel are screened before being granted access to customer data to the extent permitted by local law. *[CONFIRM: background/reference screening is actually performed — security questionnaires ask for this specifically.]*

7. International transfers

BIOPTIC is a US company and our production infrastructure is operated in the United States on Google Cloud Platform. Members of our delivery and engineering teams, and our authorised partner organisations, may access information from the countries in which they are located in order to provide the service. A current list of the countries from which Customer Content may be accessed is available on request at office@bioptic.io and is set out in our data processing agreement. *[CONFIRM: prepare this list and keep it consistent across the DPA, sub-processor list and security questionnaire answers.]*

Where personal data is transferred out of the UK, the EEA, Switzerland or another jurisdiction with transfer restrictions, we rely on appropriate safeguards — including the European Commission's Standard Contractual Clauses and the UK International Data Transfer Addendum — together with supplementary technical and organisational measures, and we carry out transfer risk assessments where required. A copy of the relevant safeguards is available on request.

For customers with data residency requirements, private cloud and on-premise deployment options are available — contact office@bioptic.io.

---

8. Retention and deletion

We keep information only as long as we need it:

Category	**Retention**
Website enquiries and sample-report requests	Up to 24 months from last contact, unless you ask us to delete earlier
Client and partner contact records	For the duration of the relationship, plus 6 years for contractual and tax records
Account and subscription records	For the duration of the subscription or licence, plus up to 12 months, then deleted or de-identified *[CONFIRM period]*

Category	Retention
Customer Content	For the duration of the subscription or engagement and while needed to support it, then deleted as set out below
Platform access, usage and security logs	Up to 12 months
Billing and accounting records	As required by applicable tax and accounting law

On written request — or following termination of a subscription or the end of an engagement — we will delete or return Customer Content within thirty (30) days, except for copies held in routine backups (deleted on our standard backup cycle of no more than [CONFIRM: e.g. 35] days), material we are legally required to retain, and de-identified material containing no customer confidential information. On request, we will confirm deletion in writing.

---

9. Security

We maintain an information security programme with administrative, technical and physical safeguards appropriate to the sensitivity of the information we hold, including:

- encryption of data in transit (TLS 1.2 or higher) and at rest (AES-256); *[CONFIRM exact standards with Ilya]*
- role-based access control, individual authentication, multi-factor authentication and single sign-on; *[CONFIRM MFA is enforced]*
- logging and monitoring of access to customer data;
- segregation of customer workspaces;
- written confidentiality obligations for all personnel, and security awareness training;
- vendor review before a new sub-processor handles customer data;
- an internal incident response process. If a security incident affects your information or Customer Content, we will notify affected customers without undue delay and cooperate with them on any regulatory notification obligations.

No system is perfectly secure, but we work to protect your information and to meet the standards our customers' security reviews require. We respond to reasonable security due diligence, and detailed security documentation is available under a non-disclosure agreement. *[Choose the statement that is accurate at publication: "We are preparing for a SOC 2 Type I examination." / once the report exists: "Our most recent SOC 2 report is available under NDA." / omit — and apply the same choice to the website's "SOC 2 in progress" placeholder.]* For

deployment options — including private cloud and on-premise arrangements — contact office@bioptic.io.

---

10. Your rights

Depending on where you live, you may have the right to:

- **access** the personal information we hold about you, and learn the categories we collect and the purposes for which we use them;
- **correct** inaccurate or incomplete information;
- **delete** your information;
- **restrict** or **object to** certain processing, including direct marketing;
- receive your information in a **portable** format;
- **withdraw consent** where processing is based on consent;
- **not be discriminated against** for exercising your rights.

If you are in the UK or EEA, you may lodge a complaint with your local supervisory authority. If you are a California resident, the rights listed above correspond to your rights under the CCPA/CPRA, including the rights to know, correct, delete, and opt out of sale or sharing; as stated in Section 5, we do not sell or share personal information as those terms are defined, and we do not use or disclose sensitive personal information for purposes requiring a right to limit. If you are in another jurisdiction, we will respond to your request in accordance with the law that applies to you.

To exercise any of these rights, write to **office@bioptic.io**. We will respond within the timeframe required by applicable law, normally within thirty (30) days. We may need to verify your identity first, and you may use an authorised agent where the law allows.

If we hold your information as a processor — because it was submitted by a customer as part of their Customer Content, or because your organisation administers your platform account — we will refer your request to that organisation and support them in responding.

---

11. Your organisation's control over accounts and content

The organisation that holds the subscription, licence or engagement controls its workspace. Its administrators may add and remove users, manage permissions, and request: a copy or export of the Customer Content we hold for them; deletion or return of that content in accordance with Section 8; and our data processing agreement, sub-processor list and security documentation, all available on request.

12. Children

Our services are for business use and are not directed to anyone under 18. We do not knowingly collect personal information from children.

---

13. Changes to this Policy

We may update this Policy from time to time. If a change is material, we will update the effective date above and give reasonable notice — by email where we hold your address, or by a notice on bioptic.io. Material changes affecting how we handle Customer Content will not apply to an active subscription or engagement without the customer's agreement.

---

14. Contact

Optic, Inc. (d/b/a BIOPTIC) 535 Mission Street San Francisco, CA 94105 United States

office@bioptic.io