PRIVACY POLICY

Effective Date: September 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 (together, the "Services").

BIOPTIC provides an agentic AI platform for the pharmaceutical and life sciences industry, available to organizations under paid licenses 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.

This Policy forms part of our Terms of Service. If your organization has a separate written agreement with us, such as 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 (or "business" under California law). Where we process Customer Content on a customer's behalf, through the platform or under an engagement, we act as a processor (or "service provider") on that customer's documented instructions, under a data processing agreement available on request.

2. What we collect

2.1 Website visitors

If you contact us through bioptic.io, by submitting a project inquiry, requesting a sample report, or subscribing to updates, we collect your business email address and any name, organization, 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 organization) for the people we work with, along with correspondence, contract, and billing records.

2.3 Accounts and subscriptions

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

- name, business email, organization, 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 third-party payment processor; we do not store full card numbers.

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 Services, 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 Services to that customer.

Regulated data. The Services are not designed to process patient-level personal data, identifiable health information (including protected health information under HIPAA), or other special-category personal data, and we do not accept such data. Our Terms of Service prohibit submitting it, we do not act as a HIPAA business associate, and our Services do not require personal data beyond business contact details. If we become aware that such data has been submitted, we may remove it and will inform the customer.

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

Purpose	Legal basis (UK/EU GDPR)
Responding to inquiries and sending requested materials	Legitimate interests; consent where required
Creating and administering accounts, subscriptions, and licenses	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
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 analyze 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 analyze 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 Services, 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. We maintain records of the contractual terms and configuration settings that apply to each provider and make them available to customers for review as part of security due diligence.

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 behavioral 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 Services, 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.

Each service provider that handles customer data is assessed before it is engaged and operates under a written agreement that includes confidentiality and data protection obligations. 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 authorized BIOPTIC personnel who need it to provide or support the Services: the delivery team assigned to an engagement, the experts who review output

before it is delivered, 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 with multi-factor authentication, logged, reviewed on a regular schedule, and revoked promptly when a person's role changes or ends. Everyone with access is bound by written confidentiality obligations, and personnel undergo background and reference screening before being granted access to customer data, to the extent permitted by local law.

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, engineering, and support teams access information from the United States and the United Arab Emirates in order to provide the Services. The complete and current list of countries from which Customer Content may be accessed is set out in our data processing agreement and is available on request at office@bioptic.io. Where an authorized partner organization is engaged for a customer, the countries from which it accesses that customer's Customer Content are included in the list provided to that customer.

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 organizational 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 inquiries 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 license, plus up to 12 months, then deleted or de-identified
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

Category	Retention
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 thirty-five (35) days), material we are legally required to retain, and de-identified material containing no customer confidential information. Customer Content remains available for export for thirty (30) days after termination, as described in our Terms of Service. On request, we will confirm deletion in writing.

9. Security

We maintain an information security program 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);
- role-based access control, individual authentication, multi-factor authentication enforced for all personnel, and single sign-on for customer accounts;
- logging and monitoring of access to customer data;
- segregation of customer workspaces;
- written confidentiality obligations for all personnel, pre-access screening, and security awareness training;
- vendor review before a new sub-processor handles customer data;
- routine backups, retained for no more than thirty-five (35) days, and documented backup and recovery procedures;
- a documented 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. We are preparing for a SOC 2 Type I examination. 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 authorized 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 organization administers your platform account, we will refer your request to that organization and support them in responding.

11. Your organization's control over accounts and content

The organization that holds the subscription, license, 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