SearchSync Privacy Policy

Version: 1.1
Effective Date: October 7, 2026
Last Updated: October 7, 2026
Posted at: https://www.searchsync.com/legal/privacy-v1.1

Introduction

SearchSync Technologies, Inc. ("**SearchSync**," "**we**," "**us**," or "**our**") operates SearchSync, a platform for the entrepreneurship-through-acquisition ecosystem, available at https://www.searchsync.com (the "**Platform**").

This Privacy Policy explains what information we collect, how we use and share it, how long we keep it, how we protect it, and what choices you have.

Two different roles. Much of the information in the Platform is not about you, it is information our customers upload about their own funds, investors, limited partners, searchers, and target companies. Where we hold information because a customer put it there, we act on that customer's instructions and the customer decides how it is used. Where we hold information about our own account holders and website visitors, we decide. Section 9 explains what this means for requests about your information.

If you are in the Beta Program. Some customers access SearchSync through an invitation-only Beta Program under a Beta Program Rider to our Terms of Service. Paragraphs in this Policy headed "Beta Program" apply only to those customers, and some processes described here are still maturing for them.

---

1. Information We Collect

1.1 Account Information

When an account is created we collect: full name; business email address; phone number; company or organization name; role or title; and the names of investment vehicles or entities associated with the account.

1.2 Billing and Payment Information

When a customer subscribes to a paid plan we collect: billing contact name and email; billing address; the last four digits and expiration date of a payment card, or the last four digits of a bank account for ACH; and transaction history, invoices, and payment status.

We do not collect or store full payment card numbers or card security codes. Payment information is collected and stored by Stripe, our payment processor, through Stripe-hosted payment components. Stripe's handling of that information is governed by Stripe's own privacy policy.

1.3 Investment, Fund, and Entity Data

When customers use the Platform they submit information including: entity and fund names and types; investment amounts, dates, and ownership percentages; capital committed, called, and deployed; ledger entries, valuation marks, and cap table data; limited partner names, contact details, and capital account information; searcher names, contact details, and fund details; target and portfolio company information; notes, tags, comments, and task lists; and performance data.

Much of this information relates to individuals who are not our account holders, for example, a customer's limited partners or the searchers in a customer's pipeline. We process that information on the customer's behalf.

1.4 Documents and Files

Customers may upload documents including: private placement memoranda; confidential information memoranda and deal materials; periodic investment updates; board reports and presentations; financial statements; operating metrics; tax documents including K-1s; and email attachments.

We process uploaded documents using AI to extract information and generate records, where the customer has enabled that feature.

What should not be uploaded. Do not upload to the Platform: information protected by HIPAA; payment card data outside the Stripe payment flow; information about children under 18; or personal information of third parties that you do not have the right to provide to us and to have processed as described in this Policy. We cannot control what customers choose to upload, and customers are responsible for the content they submit.

Tax identifiers. Tax documents such as Schedules K-1, and fields the Platform provides for investor tax information, may contain Social Security numbers, individual taxpayer identification numbers, or employer identification numbers. Where the Platform stores a taxpayer identification number in a field it designates for that purpose, the number is encrypted and displayed only as its last four digits. Access is limited to personnel whose role requires it. We do not use taxpayer identification numbers for any purpose other than providing the Platform to the customer, and we do not include them in de-identified data. Where a customer has enabled AI processing for a document containing a taxpayer identification number, the document is processed by the AI provider listed in Section 3.1, which is contractually prohibited from using it to train models.

1.5 Email Sent to Investment Addresses

Each investment or record in the Platform may be assigned a dedicated email address. When mail is sent to one of those addresses we collect the message content, attachments, and metadata including sender, recipient, and timestamps, and we process it using AI to extract information and generate records where the customer has enabled that feature.

Note for senders. A person who sends mail to a Platform address, for example a portfolio company CEO sending an update to an investor, should understand that the message and its attachments will be stored and processed in the customer's account, and that the customer, not SearchSync, decides how they are used and how long they are kept. SearchSync handles them on that customer's instructions. We may filter, quarantine, or reject messages we reasonably believe are malicious, unsolicited at volume, or unlawful.

1.6 Technical and Usage Information

We automatically collect: IP address; browser type and version; operating system; device type; approximate location derived from IP address; pages and features accessed; time spent and navigation paths; actions taken in the Platform; in-Platform search queries; errors encountered; performance metrics; and login and logout times and session duration.

Session recording. We use a third-party product analytics service, PostHog, to record interactions with the Platform so that we can reproduce defects and understand how features are used. These recordings are processed and stored by PostHog on our behalf.

How we limit what recordings capture. Session recording in the authenticated Platform is configured so that:

- all text is masked, so that investment, fund, entity, limited partner, valuation, and other data displayed on screen is replaced with placeholder characters rather than recorded;
- all form inputs are masked, including anything typed into a field;
- document viewers, file previews, and upload previews are excluded from capture entirely; and
- the contents of network requests and responses, and identifiers appearing in URLs, are redacted or not captured.

The result is a recording of how a person moved through the Platform, not a recording of the data they were looking at. We use recordings only to diagnose defects and improve the Platform, and we do not use them to monitor individuals.

Your choice. If you would prefer that we not record sessions for your account, email info@searchsync.com and we will disable it for your organization.

1.7 Cookies and Similar Technologies

Essential cookies support authentication, session management, security, and preferences. The Platform cannot function without them.

Analytics cookies help us understand feature usage, navigation, performance, and errors.

Advertising cookies, marketing website only. We may use advertising and attribution cookies on our public marketing website to measure campaign effectiveness. We do not use advertising cookies within the authenticated Platform.

Third-party services we use, including Clerk for authentication, may set their own cookies. Most browsers accept cookies by default and allow you to decline them; declining essential cookies will prevent the Platform from working.

1.8 Information from Third Parties

We receive information from: Clerk, when a user authenticates; Google Workspace, in connection with mail sent to Platform addresses; Stripe, regarding payment status and outcomes; and analytics providers, in aggregate form.

---

2. How We Use Information

2.1 To Provide the Platform

To create and administer accounts; authenticate users and manage access; store and process customer data; generate dashboards, analytics, and reports; operate AI features the customer has enabled; route and process mail sent to Platform addresses; produce exports; process payments and manage billing; and provide onboarding and support.

2.2 AI Processing

We use AI models to extract data from documents, generate records and ledger entries, summarize updates, categorize transactions, and power conversational query features.

Our commitments on AI and your data:

- **Customer data is not used to train any third-party commercial AI model,** and we do not permit our AI providers to train their models on data we submit.
- We may use **de-identified data** to train and evaluate our own internal models. See Section 4.
- AI processing can be **disabled on a per-investment or per-record basis** where the Platform supports it. Disabling it means records are entered manually.
- AI output can be incorrect or incomplete and must be independently verified before use. Our Terms of Service address this.

Our current AI provider is Anthropic. We also operate our own orchestration systems and may develop our own models.

2.3 To Communicate

To send service and security notifications, respond to support requests, and communicate with Beta Program participants about testing, features, and program updates. You may unsubscribe from those communications

at any time, using the link in each message or by emailing info@searchsync.com, and we will continue to send service and security notifications. You may opt out of marketing communications at any time without affecting service notifications. Any beta participation obligations are set out in the Beta Program Rider, not in this Policy.

2.4 To Improve and Secure the Platform

To analyze usage, diagnose defects and performance problems, test features, conduct product research, detect and prevent fraud, abuse, and security incidents, monitor for unauthorized access, maintain audit logs, investigate suspected violations of our Terms, and protect the rights and safety of SearchSync, our customers, and the public.

We use Google Analytics on our marketing website and PostHog for product analytics.

2.5 To Comply with Law

To comply with applicable law and legal process, respond to lawful requests from authorities, enforce our agreements, resolve disputes, and establish or defend legal claims.

---

3. How We Share Information

We do not sell personal information. We do not share personal information with third parties for their own marketing purposes, and we do not share it with data brokers.

3.1 Service Providers

We share information with providers who process it on our behalf, under contracts that limit them to the purposes we specify and require them to protect it. Our current providers with access to Platform data are:

Provider	Purpose	Data involved
DigitalOcean	Application hosting, managed PostgreSQL production database, backups	All Platform data
Amazon Web Services	Contingent failover infrastructure	Platform data, if activated
Cloudflare	DNS, CDN, marketing website hosting	Marketing site traffic only
Clerk	Authentication, identity, multi-factor authentication	Account and login data
Anthropic	AI models for document processing and conversational features	Content submitted for processing
Google Workspace	Company email; handling of mail to Platform addresses	Email content and attachments
Google Analytics	Marketing website analytics	Website usage data
PostHog (PostHog Cloud, US region)	Product analytics and session recording	Usage and event data; masked session recordings
Stripe	Payment processing	Billing and payment data
GitHub	Source control and deployment automation	No customer data
1Password	Credential management	No customer data

We maintain this list and give customers at least thirty (30) days' notice before engaging a new provider that will have access to customer data.

3.2 Business Transfers

If SearchSync is involved in a merger, acquisition, financing, asset sale, or bankruptcy, information may be transferred as part of that transaction. We will notify affected customers by email or prominent notice before information becomes subject to a materially different privacy policy.

3.3 Legal Requirements

We may disclose information where we believe in good faith it is necessary to comply with law or legal process, respond to a lawful request from a government or regulatory authority, enforce our agreements, protect the rights, property, or safety of SearchSync, our customers, or the public, or prevent or investigate fraud or a security incident.

Where the information belongs to a customer's account, we will notify the customer of a legal request before responding, unless we are legally prohibited from doing so or we reasonably believe notice would create a risk of harm or obstruct an investigation. Where we can, we will seek to redirect the request to the customer.

3.4 With Consent

We share information with third parties where you direct or consent to it.

3.5 De-Identified Data

We may share de-identified data as described in Section 4.

---

4. De-Identified and Aggregate Data

What it is. De-identified data is data derived from Platform data from which all direct identifiers and all reasonably identifying characteristics of a customer, its users, its funds and entities, its limited partners, its searchers, and any target or portfolio company have been removed, so that it cannot reasonably be used to identify any of them.

What we do with it. We use de-identified data to operate, secure, and improve the Platform, to train and evaluate our own internal models, and to develop industry benchmarks and aggregate insights.

Our limits:

- We do not attempt to re-identify de-identified data and do not permit anyone else to do so.
- **We do not publish or disclose any benchmark, statistic, or aggregate derived from fewer than five distinct customers.**
- We do not use customer data to train third-party commercial AI models.
- **We do not name a customer, or any of its funds, entities, limited partners, searchers, or portfolio companies, in any published benchmark, case study, marketing material, or customer reference without that customer's prior written consent.**

---

5. Security

5.1 Measures

We maintain the safeguards described in the SearchSync Security Overview, which is incorporated into our Terms of Service and which includes: TLS for data in transit and AES-256 or stronger for data at rest; encrypted database connections and backups; required multi-factor authentication for all Company personnel and for all customer users, except where a Beta Program Rider makes it optional; individual

named accounts with role-based, least-privilege access; credentials held in an approved password manager with restricted production vaults; access reviews on role change and prompt revocation on separation; automated vulnerability scanning of containers and dependencies on each deployment; security-focused code review; application, infrastructure, and database logging with anomaly detection; endpoint protection and full-disk encryption on devices accessing customer data, with endpoint detection and response in deployment; annual security and phishing-awareness training; and vendor security review before granting access to confidential information.

5.2 Backup and Recovery

We maintain daily automated database backups with point-in-time recovery within the available recovery window, currently seven days. Backups are encrypted and held separately from ordinary production access. Security and audit logs are retained up to 400 days depending on type; application, system, and access logs are retained 30 to 90 days.

We maintain a written business continuity and disaster recovery plan with a recovery time objective of one business day and a recovery point objective of up to four hours of production data loss.

5.3 Incident Response

We maintain a written incident response plan, effective August 17, 2026, owned by our Information Security Officer, with named primary and backup incident contacts. It requires immediate reporting of suspected incidents, evidence preservation, containment, investigation, documented remediation, and post-incident review, and it requires us to engage qualified legal counsel where notification or regulatory obligations may apply.

Our Terms of Service commit us to notify an affected customer without undue delay, and in any event within 72 hours after we confirm a security incident affecting their data. We will also notify individuals and authorities where applicable law requires it.

5.4 Security Limitations

We are not currently SOC 2 certified. No method of transmission or storage is completely secure, and while we work to protect information we cannot guarantee absolute security. **Beta Program.** The safeguards described in the SearchSync Security Overview apply in full during the Beta Program, except where a Beta Program Rider expressly modifies one, as it does for multi-factor authentication.

5.5 Your Responsibilities

Keep credentials confidential; use strong, unique passwords; keep multi-factor authentication enabled; protect your devices; do not share accounts; log out of shared devices; and notify us promptly at info@searchsync.com if you suspect unauthorized access.

---

6. Retention and Deletion

Active accounts. We retain account and Platform data while the account is active. Customers can access, correct, and delete most data directly in the Platform.

After termination. For sixty (60) days after a subscription ends we provide read-only access sufficient to export data, unless the subscription ended because of the customer's breach or non-payment, as set out in Section 14.5 of our Terms of Service. We delete customer content within thirty (30) days after that export window closes, and will confirm deletion in writing on request.

On request. We delete data on a customer's request within thirty (30) days, subject to the exceptions below.

Backups and logs. Data included in a backup created before a deletion request is deleted when that backup expires, currently within seven days. Logs are retained on the schedules in Section 5.2.

Exceptions. We may retain information longer where required by law, subject to a legal hold, necessary to prevent fraud or abuse, in the form of de-identified data, or held in routine backups until they expire.

Recordkeeping is your responsibility. The Platform is not an archival or compliance recordkeeping system, and we do not undertake to retain your data beyond the periods described above. You are responsible for determining which recordkeeping, retention, tax, audit, and regulatory obligations apply to you, and for exporting and retaining copies sufficient to meet them.

Beta Program. The Platform is pre-release software. The Beta Program Rider describes when we may reset the Platform, the notice we will give first, and how we carry data forward at general availability.

---

7. Your Privacy Rights

We extend the following rights to everyone who asks, regardless of where you live or which privacy law applies to you.

- **Access.** Request a copy of the personal information we hold about you.
- **Correction.** Correct inaccurate or incomplete information. Most information can be edited directly in the Platform.
- **Deletion.** Request deletion of your personal information, subject to the exceptions in Section 6 and, where a customer provided the information, to Section 9.
- **Portability.** Receive your data in a portable format. Customers can export from the Platform in XLSX and PDF.
- **Opt out of marketing.** Unsubscribe from marketing communications at any time. Service and security notifications will continue while your account is active.
- **Control AI processing.** Enable or disable AI processing per investment or record where the Platform supports it.
- **No sale or targeted advertising.** We do not sell personal information and do not use it for cross-context behavioral advertising. There is nothing to opt out of.
- **Non-discrimination.** We will not deny service, charge a different price, or provide a different level of service because you exercised a right.

How to exercise a right. Email info@searchsync.com with the subject line “Privacy Rights Request.” Include your name, the email address associated with the account, the right you want to exercise, and any detail that will help us locate the information. We respond within thirty (30) days and may need to verify your identity first. If we cannot honor a request, we will explain why.

Appeals. If we decline a request and you believe that was wrong, reply to our response and ask for an appeal. A different person will review it and respond within forty-five (45) days.

---

8. Do Not Track and Global Privacy Control

We do not sell personal information or use it for cross-context behavioral advertising, so there is no opt-out for us to honor. We do not currently respond to Do Not Track or Global Privacy Control browser signals.

---

9. If a Customer Provided Your Information

If your personal information is in the Platform because one of our customers put it there, for example, because you are a limited partner in a fund an investor tracks with SearchSync, a searcher in an investor’s pipeline, or an executive at a portfolio company, **that customer, not SearchSync, decides how the information is used and how long it is kept.** We process it on their instructions.

Please direct requests about that information to the customer. If you contact us instead, we will refer your request to the relevant customer and assist them in responding, but we will not delete or alter their records on your instruction alone. We will tell you that we have referred your request.

10. Children

SearchSync is not intended for anyone under 18, and we do not knowingly collect information from children under 18. If we learn we have, we will delete it promptly. Contact info@searchsync.com if you believe we have. Customers should not upload documents containing information about children.

11. Location of Processing and International Users

United States. SearchSync is operated from the United States and information is stored and processed there. By using the Platform you consent to that transfer.

Intended geography. SearchSync is designed and tested for users in the United States and Canada.

Canada. For users in Canada, we handle personal information in accordance with the principles of PIPEDA and, where they apply, provincial privacy laws. Personal information relating to Canadian individuals is stored and processed in the United States by SearchSync and the providers listed in Section 3.1, and while it is there it may be accessible to United States courts and government authorities under United States law. Canadian individuals may request access to, and correction of, the personal information we hold about them, and may raise a concern with us at info@searchsync.com; if we do not resolve it, they may contact the Office of the Privacy Commissioner of Canada or the applicable provincial regulator. Customers established in Quebec, or whose limited partners or other individuals are located in Quebec, may have additional obligations before personal information is transferred outside Quebec, and we will provide reasonable information to support that assessment on request.

EU and UK. We do not target or market SearchSync to individuals in the European Union or the United Kingdom. **Customers are responsible for not submitting personal information of individuals located in the EU or UK to the Platform without first entering into a written data processing agreement with us.** If you require one, contact info@searchsync.com and we will put an appropriate agreement and transfer mechanism in place.

12. Other Disclosures

Not a HIPAA business associate. SearchSync is not designed for protected health information, is not a business associate, and has no business associate agreement in place. Do not upload health information.

Not a financial institution. SearchSync is not a broker-dealer, investment adviser, bank, custodian, or fund administrator, does not hold or control assets, and does not provide investment, legal, tax, or accounting advice.

Accuracy. We rely on you to provide accurate information, to keep account details current, and to verify AI-generated output. We are not responsible for inaccurate information you provide or upload.

Beta Program. By participating in the Beta Program you understand that the Platform is pre-release; that usage analytics collection is extensive and necessary to improve the Platform; that we do not currently hold SOC 2 certification; that you should export data you want to keep; and that Beta data is intended to persist but is not guaranteed against loss.

Disputes. Disputes relating to this Policy are subject to the dispute resolution provisions of our Terms of Service, including Delaware governing law and venue and the jury trial waiver.

13. Third-Party Services

The Platform and our website may link to services we do not operate. This Policy does not apply to them. The privacy policies of our principal providers:

- Clerk, https://clerk.com/privacy
- Anthropic, https://www.anthropic.com/privacy
- Google, https://policies.google.com/privacy
- DigitalOcean, https://www.digitalocean.com/legal/privacy-policy
- Cloudflare, https://www.cloudflare.com/privacypolicy/
- Amazon Web Services, https://aws.amazon.com/privacy/
- Stripe, https://stripe.com/privacy
- PostHog, https://posthog.com/privacy
- GitHub, https://docs.github.com/site-policy/privacy-policies
- 1Password, https://1password.com/legal/privacy

---

14. Changes to This Policy

We may update this Policy. When we make material changes we will update the Last Updated date and email account holders at least thirty (30) days before the change takes effect, unless an immediate change is required for legal or security reasons. For significant changes we may require affirmative acceptance. Continued use after the effective date constitutes acceptance. Prior versions remain available at their own URLs.

If a change to this Policy is materially adverse to a customer, that customer may terminate its Order Form by written notice given within thirty (30) days after our notice, effective as of the date the change would take effect, and we will refund any prepaid, unused fees.

---

15. Contact

15.1 Privacy Inquiries and Requests

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, or wish to exercise your privacy rights, contact us at:

SearchSync Technologies, Inc.

Attn: Privacy

P.O. Box 571, Mineral Springs, NC 28108, United States

Email: info@searchsync.com (subject line: “Privacy Inquiry”)

We will respond to privacy inquiries within thirty (30) days.

15.2 Support

For general support or non-privacy questions, email info@searchsync.com or visit https://www.searchsync.com/. During the Beta Program, support is provided by email to info@searchsync.com, as set out in the Beta Program Rider.

Version 1.1 © 2026 SearchSync Technologies, Inc. All rights reserved.