

Privacy Policy

SecureThread, a product of ArcByte Studios · Version 2026-10-25

PARTICULARS	DETAILS
Document	Privacy Policy for SecureThread
Version	2026-10-25, published 25 October 2026
Provider	ArcByte Studios, a sole proprietorship of Aidan Daniel Rodrigues, registered in India as a micro enterprise under the MSME Udyam scheme
Udyam registration	UDYAM-KR-03-0759003
Registered address	GoSpace, Shelter 2, The Defence Enclave, K Narayana Pura Road, Kothanur, Bengaluru, Karnataka 560077, India
Contact	hello@securethread.co · privacy@securethread.co
Governing law	The laws of India; courts at Bengaluru, Karnataka
Online version	securethread.co/privacy-policy

This policy explains how ArcByte Studios ("ArcByte", "we"), a sole proprietorship of Aidan Daniel Rodrigues, registered in India as a micro enterprise under the MSME Udyam scheme, Udyam Registration No. UDYAM-KR-03-0759003, handles personal data when it acts as the controller under the EU General Data Protection Regulation ("GDPR") or as a Data Fiduciary under India's Digital Personal Data Protection Act, 2023 ("DPDP Act"). It covers:

- sign-up and accounts for SecureThread;
- billing contacts and billing records;
- subscribers to the status page;
- privacy requests and support requests;
- security and operational logs; and
- the cookies and browser storage that SecureThread uses.

It does not cover the content of email that a customer sends or manages through SecureThread. For that content the customer is the controller and ArcByte is its processor, under the Data Processing Agreement.

01 WHO WE ARE

ArcByte Studios is a sole proprietorship of Aidan Daniel Rodrigues, registered in India as a micro enterprise under the MSME Udyam scheme, Udyam Registration No. UDYAM-KR-03-0759003. Our registered address is GoSpace, Shelter 2, The Defence Enclave, K Narayana Pura Road, Kothanur, Bengaluru, Karnataka 560077, India. Section 12 names our Grievance Officer and privacy contact.

02 THE PERSONAL DATA WE HOLD

- 2.1 Sign-up.** The organization name, the name of the person signing up, and a work email address. We also keep a hashed form of the IP address the sign-up came from and the results of our automated sign-up checks. Where the optional bot check at sign-up (Cloudflare Turnstile) is switched on, Cloudflare receives the signals it needs to run that check. Sign-up requests that are not confirmed are deleted after 7 days. A sign-up that is used keeps these details, linked to the workspace it created, until that workspace is deleted.
- 2.2 Accounts.** Name, email address, a password stored only as a hash, a two-step verification secret stored encrypted, recovery codes stored as keyed hashes, roles, account status, sign-in history, and an optional profile photograph.
- 2.3 Sessions and security logs.** The IP address and browser user agent recorded with each session and with audit events. The audit log records security-relevant actions, such as sign-ins, changes of roles and sending actions, and it is kept for 365 days by default. A new-device alert email contains the IP address and a description of the device.
- 2.4 Billing.** The billing profile: a legal name, a billing email address, postal address and state, and a GST identification number (GSTIN) where the customer has one. Payment records held by us: amounts, dates and payment references from Razorpay. Card and bank numbers are held by Razorpay, not by us.
- 2.5 Status page subscribers.** The email address of each subscriber, whether it has been confirmed, and whether it has unsubscribed. We send a confirmation link to the address before we record a subscription as confirmed.
- 2.6 Privacy requests.** The details you give in the form: your email address, name if you give it, your relationship to SecureThread's customers, the type of request, the organization if you name one, and the details of the request. We also keep the status of the request and our notes on how we handled it.
- 2.7 Support requests.** The messages you send us through Help and support in the SecureThread app, or by writing to hello@securethread.co, and our replies.
- 2.8 Product events.** Internal records of product events, each with a name, a time and, where the event concerns a workspace, the workspace's identifier. Event properties are limited to plan names, billing periods and yes-or-no flags. They never contain email addresses, names, message content, IP addresses or user agents.
- 2.9 Server logs.** Records kept by the hosting environment, the reverse proxy and our services, which can include user IDs, email addresses, IP addresses, request times and request paths. Service logs are kept on

the server and rotate by size, so the oldest entries are overwritten by newer ones. They are not kept for a fixed period.

2.10 Browser storage. The cookies and local storage in section 6.

2.11 Notification devices. For each browser or app in which you switch notifications on: its push endpoint and encryption keys, a device label taken from its user agent, the kind of client, and the sign-in session that registered it.

2.12 Abuse reports. The details you give in the abuse report form at <https://app.securethread.co/report-abuse> or in an email to abuse@securethread.co, and our notes on how we handled the report.

03 WHY WE USE THIS DATA

3.1 We use the data above to:

- create and run accounts and workspaces;
- keep the service secure, detect misuse and investigate incidents;
- issue invoices and keep the tax and payment records we must keep;
- send status updates to subscribers who asked for them, and the email that the service needs to send, such as invitations, password resets and sign-up confirmations;
- answer privacy and support requests; and
- meet legal obligations, including requests from authorities that the law requires us to answer.

3.2 We rely on these grounds. Account, workspace and invitation emails: performance of the contract with your organization (GDPR Article 6(1)(b)), and legitimate interests (Article 6(1)(f)) where that does not apply; under the DPDP Act, a legitimate use under section 7. Security, misuse detection and incident investigation: legitimate interests (Article 6(1)(f)); under the DPDP Act, a legitimate use under section 7 and the safeguards in section 8. Invoices, tax and payment records: legal obligation (Article 6(1)(c)); under the DPDP Act, a legitimate use under section 7 for compliance with law. Status updates: consent (Article 6(1)(a)), given by confirming the subscription; under the DPDP Act, consent (section 6). Privacy and support requests: legal obligation (Article 6(1)(c)) and legitimate interests (Article 6(1)(f)); under the DPDP Act, a legitimate use under section 7. You may withdraw consent at any time: unsubscribe from status updates, or write to privacy@securethread.co for any other consent. Withdrawal does not affect processing done before it.

3.3 We do not use personal data for advertising. We do not sell personal data, and we do not share it with anyone for advertising.

04 WHO WE SHARE IT WITH

4.1 We share personal data with the service providers listed on the Sub-processors page. They process data for us under contract and only as we instruct.

- 4.2** When a customer connects its own mailbox or provider, the data in that mailbox passes between the customer, that provider and SecureThread, as the customer directs. The provider's own terms also apply.
- 4.3** We disclose personal data to authorities only where the law requires it.

05 KEEPING DATA

- 5.1** The table below gives the period for each kind of data. Where a period is not stated, we keep the data for as long as the purpose needs it, and delete it on request.

DATA	HOW LONG IT IS KEPT
Sign-up requests not confirmed	7 days, then deleted
Sessions	12 hours idle, and 14 days at most; revoked sessions are removed after one day
Audit log	365 days by default (each workspace can set 30 to 3,650 days)
Message content (body, attachments and the variables used)	180 days by default (each workspace can set 1 to 3,650 days). Message details (subject, sender, recipients, dates, status) and delivery records stay after the content is removed
Drafts not edited	90 days by default
Open and click records, when tracking is on	90 days by default; they record no IP address and no raw user agent
Delivery events reported by providers	365 days by default
Webhook payloads from providers	30 days by default; then the provider's payload is removed. A processed, ignored or failed event's record is deleted after the same period; an event still waiting to be processed keeps its record until it is processed
AI usage records, conversations and assistant memory, when those features are on	90 days by default
Notification records	30 days, except records still waiting to be sent
Mailbox watches that have been inactive	30 days
Senders, subjects and short previews of inbox mail, held to prepare push notifications	About 10 minutes in server memory; a notification showing them is stored, encrypted for the receiving device only, until the push service accepts it or it expires
Workspace after it is closed	14 days in which sign-in is refused; then, once any paid subscription has stopped, the workspace's own data is deleted. The workspace's own record remains, marked as deleted. Billing records, system emails, privacy requests and product events are kept as this table describes

DATA	HOW LONG IT IS KEPT
Status page subscribers	Kept until we delete it on request, including an address that never confirmed. Unsubscribing stops status updates.
Privacy requests	Unconfirmed requests are deleted after 7 days by an hourly job. Closed requests and their resolution notes are kept until we delete them on request.
Support requests made in the app	Deleted with the workspace
Email to hello@securethread.co and abuse@securethread.co, and abuse reports	Kept until the matter is closed, then deleted on request
Product events	Kept with the workspace's identifier only, until we delete them on request
Notification device records	Removed when you switch notifications off or sign out of the session that registered them. If that session ends another way, the record stays until you sign in on that device again
Billing payment records	Kept after a workspace is deleted, for as long as tax and accounting law requires, and deleted on request after that.
Workspace billing profile	Deleted with the workspace.
SecureThread's own system emails, including recipient addresses	While the workspace exists, a finished email's record is deleted once it is older than the workspace's audit retention period (365 days by default). After the workspace is deleted, its records are kept until we delete them on request
Backups	Default local retention 14 days. Deleted data can remain in backups for up to 14 days until those backups are replaced.

5.2 Where a law or a legal process requires us to keep a workspace's data, we may keep it beyond the periods in the table, and we do not delete it until that requirement ends.

06 COOKIES AND LOCAL STORAGE

6.1 We set the cookies below. We set no analytics cookies and no advertising cookies.

NAME	SET BY	WHAT IT IS FOR	HOW LONG IT LASTS
st_session	SecureThread	Keeps you signed in. It is HttpOnly, so scripts cannot read it. It is Secure in production and SameSite=Lax	Up to 14 days; ends after 12 hours of inactivity
st_csrf	SecureThread	Protects changes you make from cross-site requests. The page reads it by design	Until you close the browser; it stops working when your sign-in session ends

NAME	SET BY	WHAT IT IS FOR	HOW LONG IT LASTS
<code>st_sso</code>	SecureThread	Holds the state of a Google or Microsoft sign-in while it completes. HttpOnly, limited to the sign-in path	10 minutes
<code>st_sidebar</code>	The web app, when you change the sidebar	Remembers whether the desktop sidebar is collapsed	One year
<code>st_mcp_authz_</code> followed by a request identifier	SecureThread	Ties an AI assistant's connection request to the browser that started it. HttpOnly	10 minutes

6.2 Your browser also keeps a few settings and flags on your device. Apart from the client kind described after this list, none of them is sent to us:

- the theme (`st-theme`) and the reading theme of the inbox message view (`st.inbox.message-theme`);
- recent searches in the command palette (`securethread.palette.recent`);
- prompts you have dismissed: the snooze times of the AI draft banner and of the inbox permission prompt (`st.ai.draft-banner.snoozed-until` and `st.inbox.permission-prompt.snoozed-until`), and a flag that records that the Android app has asked about notifications (`st-push-app-asked`);
- whether the inbox summary is hidden (`st.inbox.summary.hidden`);
- for each person, whether notifications are switched on in this browser, with the identifier of the notification device record that this browser registered (`st-push:` and the person's identifier), and whether they were switched off here (`st-push-off:` and the person's identifier);
- for the current browsing session only: the last search in the template library (`securethread.templates.library`), the launch screen flags (`st-launch` and `st-launch-arrival`), and a mark that the SecureThread Android app started the session (`st-push-client`).

When a person switches notifications on, the browser reports its kind to us: a browser, an installed app, or the SecureThread Android app. The session mark above decides the Android app case.

6.3 We do not show a consent banner for these items. Each one is needed to provide a feature you use: keeping you signed in, protecting changes you make, remembering settings you choose, or keeping a notification device linked to your browser. If we set a cookie or browser storage item that no feature you use needs, we will ask for your consent first.

07 WHERE YOUR DATA IS STORED

7.1 Our production servers are rented from Leaseweb (Leaseweb Canada Inc.), our hosting sub-processor, and are in a data centre in Canada. The data that SecureThread itself stores is stored and processed there. Some of our service providers process personal data elsewhere, as section 7.2 describes.

- 7.2** Some of our service providers process data outside India. The Sub-processors page lists each one and where it processes data. Transfers outside India follow section 16 of the DPDP Act, which permits transfers except to countries the Government restricts by notification. For personal data of people in the European Economic Area that goes to a provider outside the EEA, we rely on the European Commission's standard contractual clauses or another mechanism that the GDPR allows.

08 SECURITY

- 8.1** We protect personal data with the measures described in the Trust page and in Annex 2 of the Data Processing Agreement. No system is completely secure. If we learn of a personal data breach that affects you, we will tell you without undue delay and in any event within 72 hours of becoming aware of it. We report the breach to the authorities as the law requires, including the Data Protection Board of India.

09 YOUR RIGHTS

- 9.1 Under the GDPR, you have the right to:**
- access the personal data we hold about you;
 - have inaccurate data corrected;
 - have data erased in the cases the GDPR allows;
 - restrict or object to some processing;
 - receive your data in a portable form, where the GDPR applies;
 - withdraw consent where we rely on it; and
 - complain to the data protection supervisory authority in the EU or EEA country where you live or work, or where the alleged infringement took place; and, where the DPDP Act allows, complain to the Data Protection Board of India.
- 9.2 Under the DPDP Act, you have the right to:**
- obtain a summary of the personal data we process and of the processing;
 - have your data corrected and erased;
 - have a grievance about processing heard and resolved; and
 - nominate another person to exercise your rights if you cannot do so yourself.

The rights in section 9.2 are set out in sections 11 to 14 of the DPDP Act. We act on a confirmed request within 30 days of receiving it. We may refuse or limit a request where the law allows, for example where we must keep records for tax or legal reasons. Make a request as section 10 describes.

- 9.3** Signed-in people can download their own data from the account's data section. Workspace administrators can export or erase a person's data or an email address's data, as the Data Processing Agreement describes.

10 HOW TO MAKE A REQUEST

- 10.1** Use the public form at </privacy/request>. You give your email address. We send a link to that address to confirm it, and we act on the request only after it is confirmed. A request is then given a reference that starts with PR-. The form asks which type of request you are making: access, correction, erasure, objection, grievance or other.
- 10.2** If your request is about email that a SecureThread customer sent you, we pass it to that customer, which is the controller of that email. We tell you by email that we have done so. That email does not name the customer.
- 10.3** We may ask you for more information to confirm who you are before we act. We respond within 30 days of receiving your confirmed request, or sooner where the law sets a shorter period.
- 10.4** Requests can also be sent by email to privacy@securethread.co. We may ask you to confirm the address before we act on an email request.
- 10.5** Some decisions are made by software. The content policy suspends a sending account after the warnings that the workspace has set, and the reputation check pauses sending when a threshold is crossed. An administrator of the workspace can reactivate a suspended account. Only ArcByte can lift a sending pause. If you think a decision about your account or sending is wrong, you can object through the form at </privacy/request>, choosing Objection, or by email to privacy@securethread.co. Objections are handled as privacy requests, and a person at ArcByte reviews each one.

11 CHILDREN

- 11.1** SecureThread is a business service for adults who act for their organization. It is not directed at children, and we do not knowingly collect the personal data of anyone under 18. If we learn that we have collected such data, we delete it. If you believe we hold a child's data, write to privacy@securethread.co.

12 GRIEVANCE OFFICER AND CONTACT

- 12.1** Our Grievance Officer, under the Information Technology Act 2000 and its rules and under the DPDP Act, is Aidan Daniel Rodrigues, Proprietor of ArcByte Studios. Write to privacy@securethread.co, or to the registered address in section 1. We acknowledge a grievance within 48 hours and resolve it within 30 days.
- 12.2** For questions about this policy or about how we handle personal data, write to privacy@securethread.co. For anything else, write to hello@securethread.co.

13 CHANGES TO THIS POLICY

- 13.1** We publish each new version with its date and a summary of the change. For a material change we give at least 30 days' notice, by email to the administrator of each workspace and in the app, and the change takes effect when that notice period ends. Continued use after that date means you accept the change, and an

administrator who does not agree may close the workspace before then. A change that only clarifies the wording or corrects an error takes effect when we publish it.

14 OUR SUB-PROCESSORS

14.1 The list of our Sub-processors, with their purposes, data and locations, is on the Sub-processors page.

This PDF reproduces version 2026-10-25 of the Privacy Policy, as published at securethread.co/privacy-policy. The online version is the authoritative one.