

Data Processing Agreement

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

PARTICULARS	DETAILS
Document	Data Processing Agreement 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/legal/dpa

This Data Processing Agreement (the "DPA") forms part of the Terms of Service between ArcByte Studios ("ArcByte") and the Customer. SecureThread is provided by ArcByte Studios, 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. Its registered address is GoSpace, Shelter 2, The Defence Enclave, K Narayana Pura Road, Kothanur, Bengaluru, Karnataka 560077, India. This DPA applies when ArcByte processes personal data on the Customer's behalf in providing SecureThread. It is written to meet Article 28(3) of the EU General Data Protection Regulation ("GDPR") where the GDPR applies, and to set out the duties of a Data Processor under India's Digital Personal Data Protection Act, 2023 (the "DPDP Act") and the Digital Personal Data Protection Rules, 2025 (the "DPDP Rules") where ArcByte acts for a Data Fiduciary.

This DPA takes effect for the Customer's workspace when an administrator of that workspace confirms in SecureThread that the Customer accepts it. ArcByte records the acceptance with the administrator's name, the version of this DPA and the time of acceptance.

01 DEFINITIONS AND ROLES

- 1.1** **Customer Data** means personal data that ArcByte processes for the Customer in the Service: messages and attachments, recipient details, contacts, templates, approvals, sign-in accounts of Users that an administrator creates, changes or erases, data fetched from the Customer's connected mailboxes on request, and AI requests made in the Customer's workspace.
- 1.2** For Customer Data, the Customer is the controller under the GDPR and the Data Fiduciary under the DPDP Act. ArcByte is the processor under the GDPR and the Data Processor under the DPDP Act.
- 1.3** Account, sign-up, billing and website data are not Customer Data, except the sign-in accounts of Users that a workspace administrator creates, changes or erases, which are Customer Data and for which ArcByte acts as a processor and a Data Processor. For the rest of that data ArcByte acts as a controller and a Data Fiduciary, as the Privacy Policy describes.
- 1.4** **Data Subject** means a person whom Customer Data is about. **Personal Data Breach** means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.
- 1.5** **Sub-processor** means a party that ArcByte engages to process Customer Data. The Sub-processors are listed on the Sub-processors page, which forms Annex 3.

02 SUBJECT MATTER, DURATION, NATURE AND PURPOSE

- 2.1** ArcByte processes Customer Data to provide the Service to the Customer, as Annex 1 describes.
- 2.2** This DPA applies for as long as the Customer uses the Service, and afterwards until Customer Data is deleted under section 9.

03 INSTRUCTIONS

- 3.1** ArcByte processes Customer Data only on the Customer's documented instructions. The Customer's use and configuration of the Service, and this DPA, are those instructions.
- 3.2** If ArcByte believes that an instruction breaks the GDPR, the DPDP Act or the DPDP Rules, it tells the Customer without delay. ArcByte is not obliged to check the Customer's instructions in general, and it may suspend the processing that an instruction covers until the Customer confirms that instruction in writing.

04 CONFIDENTIALITY

- 4.1** ArcByte makes sure that the people it authorizes to process Customer Data are bound by a duty of confidentiality, and it limits access to those who need it for the purposes in Annex 1.
- 4.2** Each person who processes Customer Data for ArcByte is bound by a duty of confidentiality and has access only to the extent that the purposes in Annex 1 require. Operator access to a workspace is granted only for a stated reason, with a ticket reference where one is given, for a period of between 15 minutes and 24 hours.

Each grant is recorded in ArcByte's audit log with its start and length, and an early end is recorded too. The workspace's administrators can see that access was opened, why and for how long, but not which staff member opened it.

05 SECURITY

- 5.1 ArcByte implements the technical and organizational measures in Annex 2. They are reasonable security safeguards for the purposes of the DPDP Act.
- 5.2 ArcByte may change a measure if the change does not reduce the protection that Annex 2 describes.
- 5.3 Annex 2 describes what the Service does. It does not promise a level of security that the Service does not provide, and it makes no claim to any certification.

06 SUB-PROCESSORS

- 6.1 The Customer authorizes ArcByte to use the Sub-processors listed in Annex 3.
- 6.2 ArcByte gives the Customer at least 30 days' written notice of a new or replaced Sub-processor before it begins processing Customer Data. The Sub-processors page shows the change.
- 6.3 The Customer may object to a new Sub-processor on reasonable data-protection grounds within the notice period. ArcByte considers the objection in good faith and tells the Customer in writing what it will do. If ArcByte cannot address the objection, the Customer may close the affected workspace (an administrator asks ArcByte to close it, and section 9 applies), and ArcByte then refunds the prepaid fees for the unused period. That refund is not subject to the refund request period in the Terms. Section 9 then applies to the Customer Data of that workspace.
- 6.4 ArcByte imposes on each Sub-processor data-protection duties that are no less protective than this DPA, and it remains responsible to the Customer for each Sub-processor's performance of those duties as if that performance were ArcByte's own, subject to section 13.
- 6.5 Some providers are chosen and contracted by the Customer: the mailbox providers, SMTP servers and HTTP email APIs that the Customer connects. ArcByte sends Customer Data to them only as the Customer directs, the Customer's own agreement with each provider governs how that provider processes the data, and they are not Sub-processors of ArcByte. The same applies to an AI provider that an administrator configures: the Customer holds its own account with that provider and supplies its key, and ArcByte's servers send AI requests to it only on the Customer's instruction. The Customer's agreement with that provider governs its processing, and it is not a Sub-processor of ArcByte. The Sub-processors page lists the AI providers the Service can be configured with.

07 HELPING WITH REQUESTS FROM DATA SUBJECTS

- 7.1 ArcByte helps the Customer answer requests from Data Subjects. Workspace administrators can:

- **export a person.** The export covers that person's profile and roles, sessions, connected mailboxes, messages and drafts they wrote while retention keeps the content, contacts and groups, templates they own, assistant credentials and send requests, AI memory and conversations, approvals, the system email sent to them, their support requests with the messages on them, the legal acceptances they gave, and audit events by or about them.
- **erase a person.** Erasure applies only to a deactivated account, never to the administrator carrying it out. It removes sessions, sign-in secrets, the avatar, AI memory and conversations, unsent drafts, personal contacts and groups, and assistant credentials. It revokes the person's own mailboxes at the provider where the provider allows it and deletes their stored credentials. The account is kept as "Former member" at a pseudonymous address. Their support requests stay, without their address or name, and the legal acceptances they gave show "Former member" in place of their name.
- **export an email address.** The export covers the contacts with that address and their groups, every sent message addressed to it, with the delivery events reported for it, its suppression entries, and the support requests from it.
- **erase an email address.** Erasure deletes the contacts, replaces the address in recipient records with a pseudonymous address, and purges the rendered content of those messages. The suppression entries stay, so that the address is never mailed again. Message records such as the subject, sender and dates stay as the workspace's business record. Support requests from the address keep their messages, without the address or name.

7.2 Each export and erasure is recorded in the workspace's audit log. The person and email-address exports are JSON files that contain the records named in clause 7.1 that the Service holds for that person or address. They do not include attachment files. If an administrator needs a record that an export does not contain, the administrator may ask ArcByte in writing for help, and ArcByte helps where the Service still holds the record.

7.3 Where ArcByte receives a request directly from a Data Subject about Customer Data, it passes the request to the Customer without undue delay and does not answer it for the Customer, unless the Customer instructs it to.

7.4 Requests from people whose address appears in mail that a Customer sent are answered by that Customer, as the controller of that mail.

08 PERSONAL DATA BREACH

8.1 ArcByte notifies the Customer of a Personal Data Breach affecting Customer Data without undue delay, and in any event within 72 hours, after it becomes aware of it.

8.2 The notice describes, as far as ArcByte knows at the time, the nature of the breach, the data and people likely affected, the likely consequences, and the measures taken or proposed. ArcByte updates the notice as it learns more.

8.3 Where the law places a duty to report a Personal Data Breach on ArcByte, ArcByte reports it as the law requires. Otherwise the Customer decides whether to notify a supervisory authority, the Data Protection Board of India, or Data Subjects, and ArcByte assists the Customer with those notifications as needed.

ArcByte gives the Customer the information described in clause 8.2 in time for the Customer to meet its own deadlines under the DPDP Act, the DPDP Rules and, where the GDPR applies, Articles 33 and 34 of the GDPR.

- 8.4** Where the Customer carries out a data protection impact assessment, or consults a supervisory authority before processing, about its use of the Service, ArcByte gives it the information about the Service that it reasonably needs, as Annex 2 and section 10 describe.

09 DELETION AND RETURN

- 9.1** When an administrator asks ArcByte to close the Customer's workspace, ArcByte closes it when it acts on the request, and the workspace enters a grace period of 14 days, during which sign-in is refused. At the end of the grace period, once any paid subscription has stopped, the workspace's data is deleted, except the records that clause 9.3 names. The workspace's own record remains, marked as deleted.
- 9.2** Backups keep Customer Data until they expire under the backup schedule. The default local retention is 14 days. Deleted Customer Data can remain in backups for up to 14 days until those backups are replaced. The backup script encrypts a backup with age or gpg only when it is run with an encryption option, and the script does not require encryption.
- 9.3** Some records are kept outside the workspace, as the Terms and the Privacy Policy describe: billing payment records, SecureThread's record of its own system emails, privacy requests and abuse reports about the workspace, ArcByte's internal notes and support-access records about it, product events that name it, and the workspace's own record of its deletion. ArcByte keeps them only for the reasons stated there. Billing payment records are kept for the accounting and tax purposes that the law requires, and the Service does not delete them on a set timetable. While the workspace exists, the record of system emails, including recipient addresses, is deleted once each finished email is older than the workspace's audit retention period (365 days by default). Once the workspace is deleted, that record is kept until ArcByte deletes it on the Customer's written request, as clause 9.4 describes. The workspace's own record stays, marked as deleted, and the retention job does not remove it.
- 9.4** On the Customer's written request, ArcByte deletes Customer Data earlier, or returns it, where the Service makes that possible. Customer Data is returned in the JSON exports that the Service provides: for a person or an email address as clause 7.2 describes, and for the whole workspace from its settings while it is active. During the grace period in clause 9.1, ArcByte may reinstate the workspace at the Customer's request so that it can be exported; once deleted, it cannot be returned. Any other return work may be done at a price agreed in writing before the work starts.
- 9.5** Deletion under this section 9 does not apply to Customer Data that a law, or a binding order of a court or authority in India or another applicable jurisdiction, requires ArcByte to keep. ArcByte keeps that data only for that purpose and for as long as the requirement lasts, and the deletion in this section 9 applies once it ends.

10 INFORMATION AND AUDITS

- 10.1** ArcByte makes available the information that is reasonably needed to show compliance with this DPA, and it allows audits by the Customer or an auditor the Customer appoints.
- 10.2** The frequency, notice, scope and cost of an audit, and the confidentiality of the audit material, are agreed in writing before the audit starts. ArcByte holds no third-party certification and no third-party audit report.

11 INTERNATIONAL TRANSFERS

- 11.1** Customer Data is stored on servers rented from Leaseweb (Leaseweb Canada Inc.) in a data centre in Canada. Some Sub-processors process parts of it in the locations that Annex 3 and the Sub-processors page state.
- 11.2** Customer Data is stored and processed only in the locations that clause 11.1 and Annex 3 state. ArcByte is established in India. Where the GDPR applies to a transfer of Customer Data from the EEA or the UK, including a transfer to ArcByte in India or onward to a Sub-processor outside the EEA or the UK, the transfer is made under the Standard Contractual Clauses approved by the European Commission (Implementing Decision (EU) 2021/914), with Module 2 or Module 3 as applicable, and, for transfers from the UK, under the UK International Data Transfer Addendum. Those clauses are incorporated into this DPA by reference. A transfer under the DPDP Act is made only to a country or territory that the Central Government has not restricted under section 16 of that Act.
- 11.3** The locations of Sub-processors appear in Annex 3.

12 DPDP ACT AND DPDP RULES

- 12.1** Where ArcByte processes personal data as a Data Processor for the Customer under the DPDP Act:
- it processes the data only under a valid contract with the Customer, and only for the purposes the Customer specifies;
 - it protects the data with reasonable security safeguards, as Annex 2 describes;
 - it informs the Customer of a Personal Data Breach without delay, so that the Customer can meet its own duties;
 - it erases the data when the Customer's purpose ends or the Customer instructs erasure, unless a law requires it to keep the data;
 - it helps the Customer meet its duties to Data Principals, including access, correction, erasure and grievance redressal; and
 - it observes any restriction on processing that the Central Government has notified.
- 12.2** The duties in clause 12.1 are ArcByte's duties as a Data Processor under the DPDP Act, 2023 and the DPDP Rules, 2025, and they apply as those laws come into force. The Customer, as Data Fiduciary, is responsible for its own duties under the DPDP Act, including, where it processes the personal data of a child, obtaining

verifiable consent from the child's parent or lawful guardian under section 9 of that Act. The Service is not designed for children's data, and the Customer must not use it to process that data.

- 12.3** The Customer is responsible for the lawful basis and notices it gives to Data Principals, and for its own consents and grievance handling as Data Fiduciary.

13 DURATION, LIABILITY AND GOVERNING LAW

- 13.1** Each party's total liability under this DPA is limited to the fees the Customer paid for the Service in the 12 months before the event giving rise to the claim. This limit is part of, and not in addition to, the limit in clause 14.1 of the Terms. Neither party is liable for indirect, consequential or lost-profit losses. Nothing in this DPA limits liability that the law does not allow to be limited, for example for fraud.
- 13.2** This DPA is governed by the laws of India. The courts at Bengaluru, Karnataka have exclusive jurisdiction over any dispute arising out of or in connection with this DPA.
- 13.3** If this DPA and the Terms conflict on the processing of Customer Data, this DPA prevails.

14 WHERE EACH ELEMENT OF GDPR ARTICLE 28(3) APPEARS

ARTICLE 28(3) ELEMENT	WHERE IT IS ADDRESSED
(a) processing only on documented instructions, including on transfers	Sections 3 and 11
(b) people authorized to process are bound by confidentiality	Section 4
(c) security measures under Article 32	Section 5 and Annex 2
(d) conditions for engaging Sub-processors	Section 6 and Annex 3
(e) assisting the controller with requests from Data Subjects	Section 7
(f) assisting with Articles 32 to 36 (security, breach notice, impact assessment, consultation)	Sections 5 and 8
(g) deletion or return at the end of the services	Section 9
(h) information needed to show compliance, and audits	Section 10

15 ANNEX 1: PROCESSING DETAILS

ITEM	DESCRIPTION
Subject matter	Operation of SecureThread for the Customer: email composition, approval, sending, mailbox use, scheduling, campaigns, audit and administration.

ITEM	DESCRIPTION
Duration	As set out in sections 2 and 9.
Nature of processing	Storage; cleaning and rendering of email content; sending through the providers the Customer connects; reading connected mailboxes on request; AI processing where enabled; audit logging; backup; export; erasure and deletion.
Purpose	The Customer's business email, approvals and governance of sending.
Personal data	Names and work email addresses of Users; mailbox addresses; contact details in contacts and recipient records; the content of messages and attachments, which can contain any personal data the Customer includes; IP addresses and browser user agents recorded with sessions and audit events; IP address and device description in new-device alert emails; AI requests, outputs, memory and conversations where those features are enabled; approval decisions; open and click records where tracking is enabled (these record no IP address and no raw user agent); delivery events reported by providers, including the recipient address; mailbox content fetched on request; profile photographs that Users supply; push subscription details for devices that a person registers.
Special categories	Not intended. The Customer decides what it sends and must not send special category data, as defined in Article 9 of the GDPR, or government identifiers such as Aadhaar or PAN numbers unless it has a lawful basis for doing so. The Service checks outgoing mail for some payment card numbers, Aadhaar and PAN numbers and secrets, but those checks are partial and do not replace the Customer's own checks.
Data Subjects	The Customer's Users; contacts and recipients outside the organization; people named in messages.

16 ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

These measures describe the Service as built. They do not cover every control, and none is a certification.

Access and sign-in

- Accounts are created by invitation, on the email domains that the workspace allows. An administrator can also allow accounts to be created by SCIM provisioning, or at work sign-in with Google or Microsoft for a domain the workspace has verified. Self-serve sign-up for new workspaces can be protected by Cloudflare Turnstile.
- Passwords are stored as Argon2id hashes. A password must be 12 to 128 characters.
- Two-step verification with an authenticator app is available to every User and required for administrators by default. Recovery codes are single use and stored as keyed hashes.
- Five wrong secrets lock an account for 15 minutes. The count covers passwords and two-step codes.
- Requests to sign in are rate limited by IP address and by account.
- Session tokens are random values stored only as hashes. Sessions end after 12 hours idle or 14 days in total. Deactivating a User ends its sessions.

Authorization

- Every action checks a named permission. The default is to refuse.

-
- A resource that a person may not see is reported as not found, not as forbidden.
 - When the workspace requires two-step verification for administrators (the default), administrative actions need a session that has completed it.
 - The last active administrator cannot be removed or demoted.
 - Security-relevant actions are written to the audit log.

Encryption and secrets

- Connections to the Service and to providers use TLS. Certificate checks are never disabled.
- Mailbox passwords and provider tokens, two-step secrets, OAuth client secrets, AI provider keys, webhook secrets and the content of system email are encrypted at the application level with AES-256-GCM, bound to the record they belong to.
- The encryption keys come from the server environment, not from the database.
- Encryption of message bodies, message snapshots, attachments, contacts and other stored personal data at the application level is **not** claimed. This Annex does not describe the encryption of the disks or volumes of the hosting environment.

Separation between workspaces

- Each record carries its workspace identifier. Queries and background jobs are scoped to a workspace.
- Database rules stop a record from linking to a record in another workspace.
- PostgreSQL row-level security is defined for workspace data. It binds only connections made with the Service's separate runtime database role, which the production Service does not yet use, so separation between workspaces rests on the application's workspace scoping and the database rules above until it does.

Handling of content

- Email HTML is cleaned on the server before it is stored, previewed or sent. Scripts, forms, frames, remote fonts and remote backgrounds are removed. Remote images stay in the stored HTML. The reader shows them in a person's own and shared mailboxes; when an administrator views someone else's mail, it hides them until the administrator chooses Show images.
- Previews run in sandboxed frames that run no scripts.
- ArcByte's servers do not fetch remote resources referenced by email content. The one exception: when mail from a domain passes DMARC with an enforced policy and that domain publishes a BIMI record, the servers request the mark certificate the record names, to show the sender's logo. That request carries no personal data.
- Email content is processed in isolated worker threads with time and memory limits.
- Uploads are checked for file type and size. The browser re-encodes a profile photograph, and the server removes its metadata before storing it. Where a malware scanner (ClamAV) is configured for the Service, each attachment is scanned before it is stored and an infected file is refused; otherwise attachments are recorded as not scanned.

Outbound connections

-
- SMTP connections go only to servers that an administrator has approved, and only to hosts that resolve to public addresses. The connection is made to the vetted address.
 - Plaintext SMTP is not used.

Logs and audit

- Logs are structured and redact secrets, cookies, passwords and message bodies.
- The audit log is append-only at the database level. Its retention is 365 days by default, set per workspace.

Infrastructure

- Application containers (API, worker and web) run as a non-root user, with read-only root file systems and dropped privileges. The migration job runs as a non-root user with dropped privileges, without a read-only file system.
- The database and cache containers set no-new-privileges. They are not read-only, and they drop no capabilities.
- No application container publishes a port. The reverse proxy on the host terminates TLS for the Service's public names: the web app, the API, the website and the status page.
- The database and the cache run on an internal network without internet access. The cache requires a password.
- Secrets come from the environment and are not written into images.
- The Service runs on a single host. There is no standby site or automatic failover.

Backups

- A database backup runs daily from a script. The script can encrypt the backup with age or gpg, and the default local retention is 14 days.
- Backup encryption with age or gpg is available in the backup script and is not required by it. The operations procedure calls for the encryption keys and the credential keyring to be stored apart from the backups.

Development and testing

- Dependency versions are pinned and a lockfile is committed. The repository defines a continuous integration workflow that runs the dependency audit (`pnpm audit:deps` , at moderate level and above).
- Automated tests include an authorization check across every API route. No external penetration test has been carried out.

Staff and incidents

- The Proprietor, Aidan Daniel Rodrigues, is responsible for ArcByte's response to a Personal Data Breach. ArcByte personnel may access Customer Data only for the purposes in Annex 1, and only as clause 4.2 describes. On a suspected Personal Data Breach, ArcByte records the time and the facts, contains the breach, preserves the evidence, assesses the data and people affected, eradicates the cause, recovers the Service, notifies the Customer under section 8, and reviews the cause and the follow-up actions.

Hosting: Leaseweb (Leaseweb Canada Inc.) hosts the Service on servers in a data centre in Canada.

The other Sub-processors are listed on the Sub-processors page, which forms part of this DPA. The page sets out each Sub-processor's name, purpose, data, location and status.

This PDF reproduces version 2026-10-25 of the Data Processing Agreement, as published at securethread.co/legal/dpa. The online version is the authoritative one.