

Template draft. This is standard boilerplate prepared for review. It is not legal advice. Replace every [highlighted placeholder] , confirm each statement matches how IdeaLine actually operates, have a qualified lawyer review it for your jurisdictions, and delete this notice before publishing.

Data Policy

Effective [EFFECTIVE DATE] · Last updated [EFFECTIVE DATE]

This Data Policy describes how [COMPANY LEGAL NAME] handles, protects and retains information in IdeaLine. It supplements the Privacy Policy and the Terms.

1. What data we hold

Category	Examples	Where it lives
Account	Email, display name, role, preferences	Managed database and authentication service
Workspace content	Projects, tasks, ideas, comments, approvals, labels, templates, file links	Managed database (one workspace per customer organization)
Activity log	Who did what and when, @mentions	Managed database, append-only
Share-link records	Hash of the link token, expiry, options, view count	Managed database. The link itself is never stored.
Operational logs	IP address, request and error logs	Hosting and infrastructure providers

We do not store the files you link from cloud storage. We store the link and the title you give it.

2. Ownership and use

Customer organizations own their content. We use it only to provide and secure the Service, to follow written instructions, and as required by law. We do not use customer content to train machine-learning models or for advertising. [Update this statement when AI features launch] .

3. Access control

- **Invitation only.** Only email addresses on the workspace allow-list can create an account. The database rejects any other address, even if sign-up is accidentally enabled.
- **Roles.** Owners manage the workspace; members create and edit work; viewers have read-only access. Roles are enforced in the database by row-level security, not just in the interface.
- **Isolation.** Each workspace's data is separated by row-level security policies.
- **Sessions.** Idle sessions time out automatically.
- **Staff access.** Production access is limited to personnel who need it, is logged and is reviewed [quarterly].

4. Link sharing

Members can create a read-only link to a project. To limit risk:

- Links are long random values (256 bits). Only a one-way hash is stored, so a database reader cannot reconstruct a link.
- Every link expires (24 hours to 30 days) and can be revoked immediately by a member.
- A link can be limited to title, status and due date, hiding the description and subtasks.
- A link never shows comments, linked files, assignees, other projects or the workspace.
- Each project may have at most 10 active links, and each link records a view count.
- Creating and revoking links is written to the audit log.

A link works for anyone who has it, so treat it like a password-free key and avoid sharing confidential or regulated information this way.

5. Encryption and transport

Data is encrypted in transit using TLS. Data at rest is encrypted by our infrastructure providers using industry-standard encryption. The application sends HTTP security headers including HSTS, a strict Content Security Policy and clickjacking protection.

6. Subprocessors

Provider	Purpose	Data	Location
Supabase, Inc.	Database, authentication, APIs	Account and workspace data	[REGION]

Provider	Purpose	Data	Location
Vercel Inc.	Web hosting and delivery, server functions, scheduled jobs	Technical request data; transient processing of workspace data in server functions	Global edge network
Cloudflare, Inc.	Domain name system (DNS) and, for backups, private object storage (R2)	DNS queries; encrypted backup files (unreadable without our key)	[REGION]
Stripe, Inc.	Payment processing (when billing is enabled)	Billing name, email, card brand and last four digits, plan and payment status. Full card data goes to Stripe only.	United States and global
[Email provider, e.g. Resend]	Transactional and digest email (if enabled)	Email address, notification content	[REGION]
Google, Microsoft, Dropbox, Box	Optional file pickers, used only when you choose them	Selected file name and link	Per provider

We will update this list before adding a subprocessor that handles customer data and give customers [30] days' notice of changes.

7. Retention and deletion

Data	Retention
Workspace content	Until deleted by the customer or the workspace is closed; then removed within [30] days
Activity log (full history of changes, comments, tags, approvals, exports and sign-ins)	Starter: 6 months. Team: 12 months. Studio: kept for as long as the account exists. Older entries are removed automatically each day.
Share-link records	Expired records are purged automatically after 7 days
Backups	Rolling [up to 35] days, then overwritten
Operational logs	[30 to 90] days

8. Export and portability

Your data belongs to you. People whose role includes exporting can download everything in the workspace at any time from Settings, Data and backup: a migration pack (ZIP with one CSV file per type plus a JSON backup and a README), an Excel workbook, or a JSON backup. The activity log your plan keeps can be exported on its own as Excel, CSV or JSON. Workspace admins can also schedule backup emails to people on their own team. Exports are logged. Any person can delete their own account at any time; an owner can also delete the whole workspace.

9. Backups and recovery

We back up so that no customer data is lost and so the Service can be restored if something goes wrong.

What	How
Frequency	A full backup runs every hour, on the hour (UTC).
What is included	Every table of the application database (workspaces, people, roles, projects, ideas, files links, comments, settings, share links, activity log, requests) and the list of sign-in accounts with their IDs. Not included: password hashes (they stay in the authentication provider; use its point-in-time recovery for full-fidelity restores) and linked files (we do not store files).
Protection	Compressed and encrypted with AES-256-GCM before it leaves our server. The key is held in the hosting provider's secret store and in an offline copy, never next to the backups. Access keys are limited to the backup bucket.
Where	A private bucket at a different provider (Cloudflare R2) from the database host, so one provider outage or account problem does not take both. Region: [REGION] .
Retention	Hourly copies for 35 days; one copy per day for 90 days. Older copies are deleted automatically.
Verification	Each backup is read back to confirm it was stored. A failed backup emails our team and the status page shows a warning if the last good backup is older than 90 minutes.
Restore	Restores are manual and limited to named administrators. A restore can be checked without changing anything first, and can be limited to certain tables. Website deployments are rolled back separately from version history and the hosting provider's instant rollback.
Targets	Recovery point objective: up to one hour of changes. Recovery time: [state a target once a restore drill is done] . These are internal goals, not a promise.

What	How
Deleted data	Information you delete can remain in encrypted backups until they expire (at most 90 days). It is not used for any purpose and is deleted again if a backup is restored.

[Confirm the hourly job, bucket, encryption key custody and a successful restore drill before publishing this section]

10. Security incidents

We maintain an incident response process. If a breach affects personal information we will notify affected customers without undue delay and within [72] hours of confirmation, with the information they need to meet their own obligations.

11. Compliance status

[State only what is true on the publication date. Example: "IdeaLine is built to support customers' SOC 2 and GDPR obligations. We have not yet completed a SOC 2 audit." Replace when an auditor issues a report.]

12. Requests and contact

For data access, deletion, a data processing agreement or security questionnaires, contact [PRIVACY CONTACT EMAIL]. To report a vulnerability, email [SECURITY CONTACT EMAIL].