

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.

Privacy Policy

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

This Privacy Policy explains how [COMPANY LEGAL NAME] ("IdeaLine", "we", "us") collects, uses and protects personal information when you use the IdeaLine project and content planning service at [PRODUCT URL] (the "Service").

1. Who we are

[COMPANY LEGAL NAME] is the controller of personal information described here, except where we process workspace content on behalf of a customer organization, in which case the customer is the controller and we are its processor. Our address is [REGISTERED ADDRESS]. Contact: [PRIVACY CONTACT EMAIL].

2. Information we collect

Account information

Your work email address, display name, avatar color, role in the workspace, and preferences such as time zone, date format and notification settings. Access is by invitation only; we create your account from an email address an authorized workspace owner has approved.

Workspace content

Content you or your colleagues add to the Service: projects, tasks, subtasks, ideas, comments (including @mentions), approval steps, labels, custom fields, links to files stored in third-party cloud services, and share-link settings. We store links to files, not the files themselves.

Activity records

An audit trail of actions in the workspace (for example, who created, moved, commented on or exported an item and when). How long it is kept depends on your plan: 6 months on

Starter, 12 months on Team, and for as long as you have the account on Studio.

Technical information

Our hosting and infrastructure providers automatically process IP address, browser type, device information, request time and error logs to deliver and secure the Service.

Information we do not collect

The IdeaLine application, where you sign in and do your work, uses only essential cookies and browser storage. It contains no advertising trackers and no analytics.

Website analytics (only if you allow it)

On our public marketing website (not inside the application) we use Google Analytics to understand which pages are useful. It loads **only after you choose Accept** in the banner, and you can change your mind at any time with the Cookie settings link in the footer. It involves some tracking: Google Analytics sets cookies and receives your approximate location, device, browser, pages viewed and how you arrived. Google Analytics 4 does not log or store IP addresses. We turn off Google signals and advertising features and ad personalization, and we set event data to be deleted after **[2 months]**. **We do not sell this data or any personal information to advertisers or anyone else, and we never will.** Google processes analytics data under its own terms as our service provider; see [Cookie Policy](#) for details and opt-out options.

Payments

We never collect or store payment card details. Fees are paid on pages hosted by Stripe, which keeps card data under PCI DSS Level 1; we receive only your billing name and email, card brand and last four digits, plan and payment status. See the [Payment Terms](#).

3. How we use information

- Provide, secure and support the Service, including authentication and access control.
- Show your team its own content, mentions and notifications.
- Maintain audit logs, prevent abuse and investigate security incidents.
- Communicate with you about the Service, including service notices and, if you enable them, email digests.
- Improve reliability and performance using aggregated, non-advertising diagnostics.
- Comply with legal obligations and enforce our terms.

4. Legal bases (EEA, UK and similar regions)

Where data protection law requires a legal basis, we rely on the following. You can withdraw consent at any time without affecting what happened before.

Purpose	Data	Legal basis (GDPR Art. 6)
Provide the Service, accounts, access control	Account, workspace content	Contract (6(1)(b))
Billing and tax records	Billing details, payment status	Contract; legal obligation (6(1)(c))
Security, abuse prevention, audit logs, backups	Technical data, activity records	Legitimate interests (6(1)(f)): keeping the Service and customers' data safe and recoverable
Service emails (invitations, security notices, digests you turn on)	Email address	Contract; legitimate interests
Website analytics (marketing site only)	Cookie identifiers, pages viewed, approximate location, device	Consent (6(1)(a)), given with the cookie banner
Responding to access requests and support	Contact details, message	Legitimate interests; steps before a contract

We do not make decisions about you using solely automated processing that has legal or similarly significant effects, and we do not profile you.

5. How we share information

We do not sell personal information, we do not share it for cross-context behavioral advertising, and we do not give it to advertisers. This is a standing commitment, not a setting. We share information only with:

- **Service providers (subprocessors)** that host and operate the Service, listed in our [Data Policy](#).
- **People you choose.** If you create a share link, anyone with that link can view the project it points to. See [Link sharing](#).
- **Third-party storage services** (Google Drive, Microsoft OneDrive, Dropbox, Box) only when you choose to browse or attach files from them. Their own privacy policies apply to that activity.
- **Authorities or advisers** where required by law, to protect rights and safety, or in connection with a merger or sale of the business, with notice where legally required.

6. Retention

We keep account and workspace information while your workspace is active. Owners can delete items at any time. Activity history is kept for 6 months on Starter, 12 months on Team and for as long as the account exists on Studio. Anyone can export their workspace data at any time, and any person can delete their own account from Settings, Plan and account. After a workspace is closed we delete or anonymize its content within [30] days, except for encrypted backups, which are overwritten on their normal cycle (hourly copies after 35 days, daily copies after 90 days) and are used only to restore the Service, and information we must keep for legal, tax or security reasons. If we restore a backup we delete again anything you had already deleted.

7. Security

We use encryption in transit and at rest, role-based access with database-level row security, invitation-only sign-up, session time-outs, append-only audit logging, security headers and hourly encrypted backups held with a separate provider. No system is perfectly secure, and we cannot guarantee absolute security. [Only state any certification, such as SOC 2, if you hold it and it is current] . See our [Data Policy](#).

8. International transfers

Information may be processed in countries other than where you live, including the United States. Where required, we use appropriate safeguards such as Standard Contractual Clauses. Primary data region: [REGION] .

9. Your rights and choices

You may have the rights below depending on where you live. To use any of them, email [PRIVACY CONTACT EMAIL] . We will verify your identity (usually by replying to the email address on the account), answer within the time the law sets (one month under GDPR, 45 days under CCPA) and will not discriminate against you for exercising a right. If your account belongs to an organization, we may direct your request to that organization's workspace owner because it is the controller. Much of this is self-service in Settings: export your data, edit it, delete your account.

European Economic Area, United Kingdom and Switzerland (GDPR)

Access, rectification, erasure, restriction, portability, objection (including to processing based on legitimate interests), withdrawal of consent, and the right to complain to your

supervisory authority (in the UK, the Information Commissioner's Office). [EU/UK representative or Data Protection Officer contact, if required]

California (CCPA / CPRA)

You have the right to know what personal information we collect, use and disclose; to delete it; to correct it; to opt out of the sale or sharing of personal information; to limit use of sensitive personal information; and to non-discrimination. **We do not sell or share personal information** (as those terms are defined in California law) and we do not use sensitive personal information to infer characteristics. We have not sold or shared personal information in the past 12 months. You may use an authorized agent to make a request.

Other US states

Residents of Colorado, Connecticut, Virginia, Texas, Oregon and other states with comprehensive privacy laws have similar rights of access, correction, deletion, portability and to opt out of targeted advertising, sale and profiling. We do none of those. If we deny a request you may appeal by replying to our answer, and you may contact your state attorney general.

Global Privacy Control and Do Not Track

Our marketing website treats a browser's **Global Privacy Control** signal as a request to decline analytics, so no analytics script loads and the cookie banner is not shown. We do not respond to Do Not Track, but analytics are opt-in anyway and the application has none.

California "Notice at collection"

Category collected	Purpose	Sold or shared ?	Kept for
Identifiers (name, work email, IP address)	Provide and secure the Service	No	While the account is active, then deleted (backups up to 90 days)
Customer records (billing name, plan, payment status)	Billing and tax	No	As required by tax law
Internet activity (pages viewed on the marketing site, only if you accept analytics)	Understand which pages are useful	No	[2 months]

Category collected	Purpose	Sold or shared ?	Kept for
Approximate location from IP address (analytics, only if you accept)	Aggregate reporting	No	As above
User content (projects, ideas, comments)	Provide the Service	No	Until you delete it or close the workspace
Sensitive personal information	Not collected on purpose. Please do not put it in the Service.	No	

California "Shine the Light"

We do not disclose personal information to third parties for their own direct marketing.

10. Children

The Service is for business use and is not directed to anyone under 16 (or the higher age required where you live). We do not knowingly collect information from children. If you believe a child has provided information, contact us and we will delete it.

11. Cookies and local storage

The application uses only essential cookies and browser storage; our marketing website uses optional analytics only with your consent. Details are in our [Cookie Policy](#).

12. Changes to this policy

We will post updates here and change the date above. For material changes we will give notice in the Service or by email before they take effect.

13. Contact

[COMPANY LEGAL NAME], [REGISTERED ADDRESS]. Email: [PRIVACY CONTACT EMAIL].
[EU/UK representative or Data Protection Officer, if required].