



Privacy Policy

How NNE Briefing collects, uses, shares and protects personal data in connection with the Service.

PRODUCT

NNE Briefing

PROPERTIES

nnebriefing.com · app.nnebriefing.com

EFFECTIVE DATE

16 August 2026

PRIVACY CONTACT

support@nnebriefing.com

Contents

1. Scope and roles
2. Definitions
3. Data we collect
4. How we use data
5. Legal bases
6. End Client data
7. Communications
8. Artificial intelligence
9. Cookies and similar technologies
10. Sharing and sub-processors
11. International transfers
12. Retention
13. Security
14. Your rights
15. California and similar US laws
16. Children
17. Third-party sites
18. Changes
19. Contact

This Privacy Policy (the “**Policy**”) describes how the operator of NNE Briefing (“**NNE**”, “**we**”, “**us**”) processes personal data when you visit our websites, create a workspace, use the application or API, or otherwise interact with the Service. It should be read together with the NNE Briefing Terms of Use. The former product name “Briefly” has been discontinued. The product is offered solely as **NNE Briefing**.

Controller and processor. NNE is an independent controller of account, authentication, billing and website data. For End Client records, briefing answers, files and other Customer Content, the Customer (the agency) is the controller and NNE is the processor (or “service provider”). End Clients who wish to exercise privacy rights in respect of briefing data should contact the agency that sent them the portal link.

1. Scope and roles

1.1. This Policy applies to nnebriefing.com, app.nnebriefing.com, api.nnebriefing.com, Portals hosted on NNE subdomains or Customer custom domains, transactional messages sent through the Service, and related support communications.

1.2. The Service is a business-to-business product for agencies and professional teams. It is not directed to consumers as an end-user social network. End Clients access a Portal solely via a Magic Link and do not create an NNE Briefing account.

1.3. Where NNE acts as processor, NNE processes Customer Content only to provide, secure and support the Service, in accordance with the Customer’s instructions, the Terms of Use and this Policy.

1.4. This Policy does not govern the Customer’s own privacy practices toward End Clients. The Customer is responsible for providing any notice and obtaining any consent required to collect End Client data through a Portal.

2. Definitions

Capitalized terms not defined in this Policy have the meaning given in the Terms of Use. In addition:

- **Personal Data** means information that identifies or can reasonably be linked to an individual.
- **Customer** means the agency or other professional entity that holds a Workspace.
- **User** means a person with a Workspace account (Owner, Admin or Member).
- **End Client** means a contact invited to complete a Portal via Magic Link.
- **Customer Content** means data submitted to a Workspace by Users or End Clients, including briefing answers, files, comments, logos and End Client contact details.

3. Data we collect

3.1 Account and Workspace data

When a User registers or administers a Workspace, we collect agency name, User name (where provided), email address, password (stored as a hash), authentication method, Workspace settings, team role, and records of invitations. If the User signs in with Google or Microsoft, we receive the profile identifiers and email address those providers share for the OAuth flow.

3.2 Billing data

If Customer subscribes or purchases add-ons, Stripe processes payment method, billing name, email, tax-relevant details and transaction history. NNE receives subscription status, plan tier, invoice references and limited payment metadata. NNE does not store full payment-card numbers.

3.3 Customer Content

We host data that Customer and End Clients submit, including End Client name, email and telephone number; Portal configuration; briefing questions and answers; file uploads; review comments; approval history; custom-domain and SMTP settings; API keys (shown once, then stored in a non-recoverable form where applicable); and webhook endpoints.

3.4 Communications data

We process message metadata and content necessary to send Portal invitations, reminders, review notices, team invites, verification and password-reset emails, storage alerts, support tickets and optional SMS or WhatsApp messages. Unsubscribe tokens and channel preferences are stored so that opt-outs can be honored.

3.5 Technical and security data

We automatically collect IP address, browser and device type, approximate location derived from IP, timestamps, request logs, cookie identifiers, CSRF tokens, and diagnostic events required to operate, secure and debug the Service. Cloudflare Turnstile may process a challenge token on registration and other sensitive flows.

3.6 Support and contact forms

If you contact us (including via Contact Us), we collect the information you submit, typically name or agency name, email address and message content, and may retain correspondence.

3.7. We do not intentionally collect special-category data (such as health, biometric or political data). If Customer or an End Client inserts such data into a briefing or file, Customer is solely responsible for a lawful basis to do so.

4. How we use data

We use Personal Data to:

- create and authenticate accounts and maintain sessions;
- provide Portals, Magic Links, autosave, review workflows and file storage;
- send transactional and reminder communications that Customer enables;
- process subscriptions, add-ons, invoices and failed-payment recovery;
- enforce plan limits, seats, storage quotas and usage credits;
- operate AI features that Customer or an End Client invokes;
- deliver API and webhook events that Customer configures;
- provide support, investigate abuse and protect the security of the Service;
- comply with law, enforce the Terms of Use and respond to lawful requests; and
- improve reliability and product quality, using aggregated or de-identified information where practicable.

We do not sell Personal Data. We do not use Customer Content to train generalized public models for unrelated third parties. Text sent to contracted AI providers is processed to fulfill the specific request, as described in Section 8.

5. Legal bases

Where the GDPR or UK GDPR applies to NNE as controller, we rely on one or more of the following bases:

PURPOSE	TYPICAL LEGAL BASIS
Account creation, authentication and Service delivery	Performance of a contract
Billing, invoicing and fraud prevention	Contract; legitimate interests; legal obligation
Security, CSRF, rate limiting and abuse prevention	Legitimate interests; legal obligation
Transactional email and in-product notices	Contract; legitimate interests
Optional marketing communications (if any)	Consent, or legitimate interests where permitted, with opt-out
Compliance with law and legal claims	Legal obligation; legitimate interests

Where NNE acts as processor, the Customer is responsible for establishing the legal basis for End Client and briefing data (typically the Customer's contract with the End Client, legitimate interests, or consent).

6. End Client data

6.1. End Clients do not register with NNE. Their Personal Data is entered by the Customer or by the End Client in a Portal. Anyone in possession of the Magic Link can open that Portal. The Customer must treat the link as an access credential.

6.2. NNE processes End Client data only as processor, to host the Portal, store answers and files, send reminders that the Customer enables, and display review status to the Customer's Users.

6.3. End Client requests to access, correct or delete briefing data should be sent to the Customer. NNE will provide reasonable assistance to the Customer, including by implementing deletion when the Customer deletes a client, Portal or Workspace.

6.4. Deleting an End Client in the Service also deletes Portals attached to that End Client. That action is irreversible, subject to residual backups retained for a limited period.

7. Communications

7.1. We send service emails that are necessary to operate the account (verification, password reset, team invitations, billing notices and security alerts). These are not marketing messages.

7.2. Portal invitations, incomplete-briefing reminders and review notices are sent on the Customer's instruction. Incomplete-briefing reminders, where enabled, are sent at most three times per Portal and cease if the trial or paid Plan ends.

7.3. SMS is delivered through Amazon SNS (or an equivalent provider). WhatsApp is delivered through Meta WhatsApp Cloud API using approved templates. Both consume Customer messaging credits and are unavailable during the free trial. The Customer must have a lawful basis to send those messages, including consent where required by the Telephone Consumer Protection Act or similar law.

7.4. End Clients may opt out of reminder emails, SMS and WhatsApp via the unsubscribe link in the message footer. We honor those preferences for subsequent reminder traffic on the same channel.

7.5. If Customer uses its own SMTP, Customer is the sender of record. NNE processes SMTP credentials solely to transmit messages on Customer’s behalf and does not warrant deliverability of Customer’s mail infrastructure.

8. Artificial intelligence

8.1. Optional AI features include question suggestions for Customer and answer assistance for End Clients. Use is subject to Plan and add-on limits.

8.2. Prompts and relevant briefing context may be transmitted to OpenAI (or a successor provider) solely to generate the requested output. That provider processes the data as NNE’s sub-processor for that request.

8.3. AI output may be inaccurate. It does not replace human review. Customer and End Clients remain responsible for any text they accept or submit.

8.4. Customer should not submit secrets, payment-card data or special-category data to AI features unless it has a documented lawful basis and accepts the additional risk of transmission to the model provider.

9. Cookies and similar technologies

9.1. We use cookies and similar technologies that are strictly necessary to operate the Service. We do not use advertising or cross-site tracking cookies.

COOKIE / TOKEN	PURPOSE	TYPICAL LIFE
nne_auth	Authenticated session for Users	7 days
nne_csrf	Cross-site request forgery protection	7 days
nne_oauth_setup	Completing Google or Microsoft registration	15 minutes
Cloudflare Turnstile	Bot protection on registration and sensitive flows	Challenge / session, as set by Cloudflare

9.2. Magic Links are URL credentials, not cookies. They permit Portal access without an End Client account. Customer controls distribution of those links.

9.3. Browsers may allow Users to block cookies. Blocking strictly necessary cookies will prevent sign-in and other core functions.

10. Sharing and sub-processors

10.1. We share Personal Data only as described in this Policy, with Customer’s Users as needed to operate the Workspace, or as required by law.

10.2. We use sub-processors to host and operate the Service. Typical categories and current providers include:

PROVIDER	FUNCTION
Hosting / database providers	Application hosting and PostgreSQL storage
Cloudflare (including R2 and Turnstile)	CDN, object storage for files, bot protection
Stripe	Payments, invoices and tax-related billing data
OpenAI	AI question suggestions and answer assistance
Amazon SNS	SMS delivery
Meta Platforms	WhatsApp Cloud API
Email delivery providers	Transactional mail from the NNE sender
Google / Microsoft	OAuth sign-in, if the User elects that method

10.3. If Customer enables integrations (including Slack, Trello, Asana, monday.com, HubSpot, Zapier, Make, the API or webhooks), Customer instructs NNE to transmit the relevant data to those destinations. Those third parties process data under their own terms. Customer is responsible for what it sends.

10.4. We may disclose data to professional advisers, or to a successor in a merger, acquisition or asset sale, under confidentiality obligations. We may disclose data if required by law, court order or competent authority, or to protect the Service, Users or End Clients from serious harm.

11. International transfers

11.1. The Service is offered to Customers worldwide. Infrastructure and sub-processors may be located in the United States, the European Economic Area or other countries.

11.2. Where Personal Data is transferred from the EEA, United Kingdom or Switzerland to a country that has not been recognized as providing adequate protection, we rely on appropriate safeguards, such as the European Commission's Standard Contractual Clauses (and the UK international data transfer addendum, where applicable), together with supplementary measures as required.

11.3. By using the Service, Customer instructs NNE to make such transfers as are necessary to provide the features Customer enables (including AI, SMS, WhatsApp, storage and payment processing).

12. Retention

12.1. Account and Workspace data are retained for the life of the Workspace and for a reasonable period thereafter as needed for billing, security logs, dispute resolution and legal compliance.

12.2. Team activity history and Portal review history are retained in the product interface for thirty (30) days, after which those event records may be deleted, unless a longer period is required to operate a specific feature.

12.3. Files remain until Customer or an authorized User deletes them, the Workspace is deleted, or storage is otherwise purged after account closure. Soft-deleted files may remain listed as removed for audit on the Portal.

12.4. If the Owner deletes the account, the Workspace — including clients, Portals, briefings and files — is permanently deleted, subject to residual backups retained for a limited period and any legal hold.

12.5. Billing records and tax-relevant data may be retained for the period required by applicable accounting and tax law.

12.6. After a trial ends without a paid Plan, NNE may restrict the Workspace and, after reasonable notice, delete data in inactive or unpaid Workspaces.

13. Security

13.1. We maintain commercially reasonable technical and organizational measures, including encryption in transit, access controls, hashed passwords, CSRF protection, rate limiting and HMAC signing of webhooks.

13.2. No method of transmission or storage is perfectly secure. Customer shall use strong passwords, protect Magic Links and API keys, revoke unused invitations, and keep devices updated.

13.3. We will notify Customer without undue delay of a personal-data breach affecting Customer Content, and will notify individuals or authorities where legally required.

14. Your rights

14.1. Subject to applicable law (including the GDPR and UK GDPR), Users may request access, correction, deletion, restriction, portability, and objection to certain processing, and may withdraw consent where processing is based on consent.

14.2. Users may update certain profile and Workspace information in Settings. Account deletion is available in account settings, as described in the Terms of Use.

14.3. To exercise rights regarding User account data, email support@nnebriefing.com from the registered address. We may need to verify the request. We will respond within the period required by law.

14.4. End Clients should contact the Customer (the agency) for requests about briefing answers, files or contact details stored in a Workspace. NNE will assist the Customer as processor.

14.5. You may lodge a complaint with a supervisory authority in your country of residence, place of work or place of the alleged infringement. We encourage you to contact us first so that we can attempt to resolve the matter.

15. California and similar US laws

15.1. If you are a California resident, the California Consumer Privacy Act (as amended by the CPRA) may grant you the right to know, delete, correct and opt out of “sale” or “sharing” of personal information, and the right not to be discriminated against for exercising those rights.

15.2. We do not sell personal information and we do not share it for cross-context behavioral advertising. We process Customer Content as a service provider / processor on the Customer's behalf.

15.3. Categories of personal information we collect are described in Section 3. We collect them from you, from your Users and End Clients, from payment and authentication providers, and automatically from your device.

15.4. Authorized-agent and appeal procedures, where required, may be initiated through support@nnebriefing.com. Similar rights may exist under other US state privacy laws; we will honor applicable

requests as required.

16. Children

The Service is intended for professional use by adults. It is not directed to children under 16, and we do not knowingly collect Personal Data from children. If you believe a child has provided data to us, contact support@nnebriefing.com and we will take appropriate steps to delete it.

17. Third-party sites

The Service may contain links to, or integrations with, third-party sites and applications. Their privacy practices are governed by their own policies. NNE is not responsible for those practices.

18. Changes

We may update this Policy to reflect legal, product or operational changes. The current version will be published with its effective date. Material changes will be notified by email or in-product notice with reasonable advance notice where practicable. Continued use after the effective date constitutes acceptance of the updated Policy.

19. Contact

Privacy inquiries, data-subject requests concerning User account data, and notices to NNE:

- Email: support@nnebriefing.com
- Website: <https://nnebriefing.com>
- Application: <https://app.nnebriefing.com>
- API: <https://api.nnebriefing.com>

Until a dedicated data-protection officer is designated, the same address serves as the privacy contact. End Client requests about Portal content should be directed to the Customer that operates the Workspace.

Effective date: **16 August 2026**. Version **1.0**.

NNE Briefing — Privacy Policy v1.0 · 16 August 2026 · support@nnebriefing.com · Read together with the Terms of Use.
English is the controlling language.