Privacy Policy

American English version

Version dated October 5, 2026

GROUPE GARAN · tonaily.com · contact@tonaily.com

Contents

1 Scope and data controller . . . 2
2 Data processed and its sources . . . 2
3 Purposes and legal bases . . . 3
4 Specific rules for Google user data . . . 4
5 Artificial intelligence features . . . 5
6 Teams, CMS platforms, and connected agents . . . 5
7 Data recipients . . . 6
8 Transfers outside the European Economic Area . . . 6
9 Retention periods and deletion . . . 7
10 Cookies and other tracking technologies . . . 7
11 Security and confidentiality . . . 8
12 Your rights and how to exercise them . . . 8
13 Users who are minors . . . 9
14 Updates and language versions . . . 9

1 Scope and data controller

This Policy explains how personal data is processed when you visit tonaily.com, use the app.tonaily.com platform, or communicate with Tonaily. Personal data is information relating to an identified or identifiable individual. Truly anonymous statistics that no longer allow an individual to be identified do not fall within this definition.

GROUPE GARAN, a French simplified joint-stock company (société par actions simplifiée, or SAS) with share capital of EUR 100, registered with the Paris Trade and Companies Register under SIREN number 953 558 582, with its registered office at 200 rue de la Croix Nivert, 75015 Paris, France, is the controller of the processing it determines for account management, relationships with its users, billing, support, security, and website management. In this Policy, "Tonaily" or "we" means GROUPE GARAN.

For any question or request concerning your data: contact@tonaily.com. Mailing address: GROUPE GARAN, 200 rue de la Croix Nivert, 75015 Paris, France. Telephone: +33 6 33 18 05 11.

Where Tonaily processes personal data contained in a customer's projects or content solely on that customer's behalf and on its instructions, the customer is the controller or a processor duly authorized by its own controller. Tonaily then acts as a processor or subprocessor. These operations are also governed by Annex 4 of the General Terms and Conditions: https://tonaily.com/terms/. This Policy does not replace the information the customer must provide to individuals whose data it processes.

2 Data processed and its sources

The data depends on the features you use. We receive information you provide directly, information supplied by users or administrators you authorize, data from services you connect, and technical data generated when the Service is used. Analyses may also involve public pages or information; where such information identifies an individual, it remains personal data.

Account and organization

Name, email address, information needed for authentication, organization and subscription information, invitations, and authorized users' permissions. Signing in with Google allows us to receive your name and email address. Information essential to account creation, authentication, or billing must be provided for the relevant feature to be used; integrations and project content depend on your choices.

Projects, content, and artificial intelligence features

Instructions, keywords, documents, text, information about websites being analyzed, generated content, and settings for requested operations, to the extent these items relate to an individual. This data comes from you, your team, authorized integrations, or sources used in analyses. Avoid providing unnecessary personal data or sensitive data without a need and an appropriate legal basis.

Google Search Console and other integrations

For Search Console: properties you authorize us to access, queries, pages, clicks, impressions, click-through rates, average positions, and website URLs. We receive this data through Google APIs after you authorize access. For a connected CMS or agent: data and permissions necessary for the features you enable, within the scope of the access you grant. The rules specific to Google data are set out in Section 4.

Payment and billing

Billing information, transaction references, payment status, the plan purchased, and information needed for accounting records. Payments are processed by Stripe. Tonaily does not retain your full payment card number; data needed for payment is processed by Stripe according to its role and its policy: https://stripe.com/privacy.

Usage, audience measurement, and technical data

Pages viewed, interactions with the Service, device and browser type, referring page, and technical information needed for operation, diagnostics, and security, which may include an IP address and sign-in events. Audience measurement uses self-hosted Matomo and Google Analytics. Aggregated results do not mean that all data initially collected is anonymous. The rules applicable to tracking technologies are set out in Section 10.

Support requests and chat

Contact details and messages you send us, account information needed to handle your request, and attachments you choose to provide. If you start a conversation through the website's chat, Tawk.to processes your messages and technical context data, including your browser and pages visited. Its policy is available here: https://www.tawk.to/privacy-policy/. Chat data should not include sensitive information or secrets that are unnecessary for your request.

3 Purposes and legal bases

For processing for which Tonaily is the controller, the main purposes and legal bases provided for in Article 6 of the GDPR are set out below. Where we act on a customer's behalf, the purposes and legal basis of that customer's processing are the customer's responsibility; we carry out its lawful instructions.

Purpose	Legal basis
Create and administer an account; provide the subscription and requested features.	Performance of a contract or precontractual measures requested by the individual, where that individual is a party to the contract (Article 6(1)(b)). For contacts and users of a customer organization: legitimate interest in providing the Service and managing that business relationship (f).
Receive, display, and analyze Google Search Console data for authorized features.	Consent to the voluntary processing of Search Console data (a). OAuth authorization defines technical access; it does not constitute consent to all other processing described in this Policy.
Process payments and manage subscriptions.	Performance of a contract (b) or, for an organization's contacts, legitimate interest in administering the relationship (f).
Issue and retain invoices and comply with accounting, tax, and legal obligations.	Compliance with a legal obligation (c).
Provide support, handle requests, and send messages necessary for the Service.	Performance of a contract where a contractual obligation is involved (b); otherwise, legitimate interest in responding to requests and administering relationships with users (f).

Purpose	Legal basis
Secure the Service, diagnose incidents, and prevent abuse.	Legitimate interest in protecting users and the Service (f); compliance with a legal obligation where applicable (c).
Measure audience and improve the website or product.	Consent for tracking technologies that are not exempt and for processing that depends on them (a). For audience measurement that actually qualifies for an exemption, or operational data without tracking technologies subject to consent: legitimate interest in understanding and improving the Service (f).
Respond to requests to exercise rights and meet obligations imposed by competent authorities.	Compliance with a legal obligation (c).

Where we rely on a legitimate interest, we take your rights and freedoms into account and limit processing to what is necessary for the stated purpose. You may object under the conditions set out in Section 12. Where consent is required, it must be freely given, specific, informed, and indicated by an affirmative action. Simply reading this Policy or accepting the General Terms and Conditions does not constitute consent to optional processing.

4 Specific rules for Google user data

This section concerns information received when you sign in with Google or connect Google Search Console. It takes precedence over any general description of artificial intelligence features or recipients that would be inconsistent with the restrictions applicable to Google data.

Access and authorized uses

Google sign-in provides your name and email address to create your account and authenticate you. Search Console provides read-only access to the properties and performance data covered by the permissions you grant. We use this data for features visible in Tonaily: displaying search performance, building and prioritizing the keyword corpus, planning content based on queries for your websites, and measuring traffic to published content. Access is limited to information needed for these features.

Storage and sharing

Google user data is hosted on Amazon Web Services in the European Union and encrypted at rest. OAuth tokens are stored in encrypted form. We disclose this data only in circumstances permitted by Google's rules: to the hosting provider where necessary for the described features, for security and investigations of abuse, to comply with the law, or with your explicit consent where such sharing is permitted. Naming an AI provider in this Policy does not constitute general authorization to send that provider your Google data.

We do not sell Google user data, use it for advertising, share it with data brokers, or use it to assess creditworthiness or grant credit. It is not used to develop, improve, or train general-purpose artificial intelligence or machine learning models.

Human access and Limited Use

Human access to Google data is limited to circumstances permitted by Google's rules, including with your agreement to respond to a support request, where necessary for security or compliance with the law, or for permitted internal operations using aggregated and anonymized data. Tonaily's use and transfer to any other application of information received from Google APIs comply with the Google API Services User Data Policy, including its Limited Use requirements: https://developers.google.com/terms/api-services-user-data-policy.

Withdrawal of access and deletion

You can disconnect Search Console in Tonaily or revoke access through your Google account permissions: https://myaccount.google.com/permissions. Features that require this access will then stop working. Tokens that are no longer needed are revoked and deleted; the retention period for imported data does not justify retaining revoked tokens. Search Console data already imported is deleted no later than thirty days after disconnection or account deletion, whichever occurs first.

Before any new use of Google data that requires additional information or authorization, we explain the new purpose and obtain the required authorization or consent. Withdrawing consent does not affect the lawfulness of processing carried out before withdrawal.

5 Artificial intelligence features

Depending on the feature requested, Tonaily uses services from Anthropic (Claude), OpenAI (ChatGPT), Google (Gemini), and xAI (Grok). Instructions, document or content excerpts, and contextual information transmitted are limited to what is necessary for the requested generation or analysis. They may contain personal data if you include it in your content or if the information analyzed identifies an individual.

Use of these services remains subject to the applicable purposes, legal bases, data processing obligations, and transfer safeguards. Where Tonaily processes data on your behalf, Annex 4 of the General Terms and Conditions governs these operations. The specific rules in Section 4 continue to apply to Google data, including the restriction concerning general-purpose models.

Processing a provider carries out for its own purposes, where it acts as a controller, is also subject to its privacy information and applicable law. This Policy does not extend to those providers the thirty-day period for deleting data retained by Tonaily. You may request information about recipients and the safeguards applicable to your data at contact@tonaily.com.

6 Teams, CMS platforms, and connected agents

Users, administrators, and agents you authorize may access project data within the limits of their permissions. You must select the people and services authorized to access the data and avoid granting broader access than necessary. Tonaily applies the access permissions granted within the Service.

Publishing to a CMS or an agent's action may transmit content or data to the connected service. Depending on the action, published content may become publicly accessible. These transmissions must correspond to the operations you authorize and remain subject to the specific restrictions applicable to Google data. The service you connect is also governed by its own terms and privacy information.

You may withdraw an integration's permissions for future operations. Withdrawing them does not automatically delete content already published or a copy received by a service to which you asked for data to be sent. Requests for deletion by that service are governed by the law and its role in the processing.

7 Data recipients

Data is accessible to Tonaily's authorized personnel and to recipients necessary for the relevant purpose. Access is limited according to the applicable roles, permissions, and confidentiality obligations.

Recipient or category	Relevant function
Amazon Web Services (AWS), including AWS Lambda.	Technical infrastructure, hosting, and execution of platform functions. Google user data is hosted in the European Union.
Anthropic (Claude), OpenAI (ChatGPT), Google (Gemini), xAI (Grok).	Artificial intelligence generation and analysis features, within the limits of Section 5 and the restrictions concerning Google data.
Google.	OAuth authentication, access to authorized Search Console APIs, and audience measurement through Google Analytics. Google's information: https://policies.google.com/privacy.
Stripe.	Payment processing and billing-related services. Its role may be that of a processor or controller depending on the operation: https://stripe.com/privacy.
Tawk.to.	Website support chat, when this feature is used: https://www.tawk.to/privacy-policy/.
Users and connected services you authorize; legally authorized public authorities.	Team sharing, requested publications and actions; disclosures required by a legal obligation, within the applicable limits.

Matomo is self-hosted: the corresponding audience measurement data remains under Tonaily's control and is not sent to Matomo as an external analytics service. We do not sell your data or disclose it to advertisers. This rule does not prevent the processing expressly described for Google Analytics, payment, or the features you use.

Providers that process data on our behalf must be subject to appropriate data protection commitments. Where Tonaily acts as a processor for your organization, changes to subprocessors also follow the rules in Annex 4 of the General Terms and Conditions.

8 Transfers outside the European Economic Area

Using international providers or services you connect may involve processing or access to data from a country outside the European Economic Area (EEA). Hosting in the European Union alone is not sufficient to rule out all access from another country.

A transfer subject to the GDPR may take place only under a valid mechanism: an adequacy decision applicable to the country, recipient, and processing concerned, or appropriate safeguards, including the European Commission's Standard Contractual Clauses and necessary supplementary measures. A recipient's actual coverage under an adequacy decision must be verified; the provider's brand name alone is not sufficient.

Where Tonaily acts as a processor, these transfers must also comply with the customer's documented instructions and Annex 4 of the General Terms and Conditions. The restrictions specific to Google data

remain applicable. You may obtain information about transfers concerning your data and a copy of the relevant safeguards by writing to contact@tonaily.com; information unrelated to your request and protected confidential information may be redacted without preventing verification of the safeguards.

9 Retention periods and deletion

Data is retained for the period necessary for the relevant purpose. Customer data retained by Tonaily is deleted no later than thirty days after account deletion, except where retention is required by law.

Data	Retention period or criterion
Account, projects, and content retained by Tonaily.	While the account is active and to the extent necessary for the Service; deletion no later than thirty days after account deletion, except where retention is required by law.
Imported Google Search Console data.	While the connection is active; deletion no later than thirty days after disconnection or account deletion, whichever occurs first. Tokens that are no longer needed are revoked and deleted in accordance with Section 4.
Accounting records and supporting documents subject to mandatory retention.	For the applicable statutory period, including ten years for accounting documents and supporting documents covered by Article L123-22 of the French Commercial Code. This data remains protected and is used for that obligation.
Support requests and technical data.	For the time necessary to handle the request, follow up on the issue, or address the relevant security matter. Where associated with a deleted account, the maximum period of thirty days applies, except where retention is required by law.
Cookies, consent choices, and audience data.	According to their function, the period necessary for that function, and the applicable legal limits. Withdrawing consent stops processing that depends on it. Truly anonymized data may be retained for statistical purposes without allowing an individual to be reidentified.

Canceling a paid subscription does not by itself delete the account. While the account remains active, including under an available free plan, data necessary for the Service may be retained. You may request account deletion at contact@tonaily.com.

Where Tonaily processes data on your behalf, its return and deletion are also governed by Annex 4 of the General Terms and Conditions. Any backup copies remain subject to the applicable deletion obligations and do not permit processing to be extended for another purpose. Processing by providers that act as controllers for their own purposes follows their legal obligations and privacy information.

10 Cookies and other tracking technologies

A cookie or other tracking technology allows information to be stored on or accessed from your device. Not all tracking technologies are necessary for the Service to function. Consent rules for tracking technologies apply in addition to the rules governing personal data processing.

Category	Function and applicable rule
Session and authentication.	Account sign-in and access security. Tracking technologies strictly necessary for the service expressly requested are exempt from prior consent.
Self-hosted Matomo.	Website audience measurement. Self-hosting alone does not create an exemption. Use without consent is permitted only where the configuration and uses actually meet the legal conditions for an exemption; otherwise, prior consent is required.
Google Analytics.	Measurement of website traffic and interactions. The corresponding tracking technologies require prior consent. Refusing audience measurement tracking technologies does not block the use of Tonaily.
Tawk.to.	Maintaining a chat conversation and continuity between pages. Only tracking technologies strictly necessary for the chat you request may be exempt; others require prior consent. Refusing chat does not block access to the Service's other features.

Tracking technologies that are not exempt must be stored or read only after you consent. You have the right to refuse as easily as you accept and to withdraw consent at any time with the same ease. Choices must relate to the relevant purposes and cannot be inferred merely from continued browsing or acceptance of the General Terms and Conditions.

Browser settings also allow you to delete or block cookies. They do not replace the obligation to obtain consent and allow it to be refused or withdrawn where required. Blocking tracking technologies strictly necessary for authentication may prevent sign-in, whereas refusing audience measurement must not prevent use of the Service. For any question about your choices or data, contact contact@tonaily.com.

11 Security and confidentiality

We implement technical and organizational measures appropriate to the nature of the data and the risks of processing, in accordance with Article 32 of the GDPR. They include TLS-encrypted connections, AWS infrastructure, restricted access to production systems, and encryption of OAuth tokens at rest. Additional commitments concerning Google data are set out in Section 4.

Access to data is restricted to authorized persons and subject to confidentiality obligations. In the event of a personal data breach, notifications to authorities, customer controllers, and affected individuals are made under the conditions provided for by the GDPR.

12 Your rights and how to exercise them

Under the conditions provided for by the GDPR, you have the following rights:

- Access to your data and information about its processing.
- Rectification of inaccurate data and completion of incomplete data.
- Erasure where the legal conditions are met.
- Restriction of processing in the circumstances provided for by law.

- Portability of data you have provided where processing is automated and based on your consent or a contract, and transmission to another controller where technically feasible.
- Objection, on grounds relating to your particular situation, to processing based on a legitimate interest. We then stop that processing unless there are compelling legitimate grounds or it is necessary for the establishment, exercise, or defense of legal claims. You may object to direct marketing at any time.
- Withdrawal of your consent at any time without affecting the lawfulness of processing before withdrawal.

You may exercise these rights by writing to contact@tonaily.com or GROUPE GARAN, 200 rue de la Croix Nivert, 75015 Paris, France. Specify your request and provide useful information for locating the data concerned. If we have reasonable doubts about your identity, we may request only the additional information necessary to confirm it; a copy of an identity document is not automatically required.

We respond without undue delay and no later than one month after receiving the request. Where justified by its complexity or the number of requests, this period may be extended by two additional months; we inform you of the extension and its reasons within the first month. Exercising your rights is generally free of charge. The GDPR exceptions for manifestly unfounded or excessive requests must be justified.

If your data appears in content processed solely on a customer's behalf, also address your request to that customer as the controller. Tonaily provides the required assistance and forwards relevant requests according to the customer's instructions and the law. If we determine the relevant processing ourselves, we remain directly responsible for responding.

You may lodge a complaint with the CNIL: https://www.cnil.fr/fr/adresser-une-plainte, or with the competent supervisory authority, including the authority for your habitual residence, place of work, or the place where you believe an infringement occurred. This right does not require you to submit a complaint to Tonaily first.

13 Users who are minors

The Service is intended for users who are at least sixteen years old. Users under eighteen must have permission from their parent or legal representative in accordance with the General Terms and Conditions; a paid subscription for a minor must be purchased by the minor's parent or legal representative. If you believe a child who does not meet these conditions has provided us with data, contact contact@tonaily.com so that the situation can be reviewed and the required measures taken.

14 Updates and language versions

We may amend this Policy to reflect changes in the Service, processing, or applicable law. Significant changes are communicated by email or a notification within the Service. The date on the first page identifies the document version. Amending the Policy does not replace consent required for a new purpose; that consent must be obtained before the relevant processing.

The Policy is available in French and American English. Both versions describe the same processing and commitments. If there is a difference in meaning, the French version prevails to the extent permitted by law, without depriving individuals of their mandatory rights. The point of contact for this Policy remains contact@tonaily.com.