

Murmurly Privacy Policy

Effective date: 28 September 2026 · Version 1.0

This Privacy Policy explains how Murmurly B.V. (“Murmurly”, “we”, “us”) processes personal data when you visit our website, use Murmurly, or otherwise interact with us.

Murmurly B.V. is established in the Netherlands. For privacy questions or requests, contact us at legal@murmurly.io.

Unless stated otherwise, references to Articles in this Privacy Policy are to the GDPR.

1. Scope and our role

Murmurly processes personal data in different roles depending on why the data is processed.

When Murmurly determines the purpose, we act as controller. This includes, for example, data relating to our website, your Murmurly account, authentication, profile and preferences, user terms and privacy acknowledgements, customer and support relationships, security and product analytics.

When a customer or other third-party organisation uses a Murmurly workspace to process personal data for its own business purposes — such as information about people, organisations, engagements, events, invitations, RSVPs, notes, tasks, agendas, feedback or files — that organisation generally acts as controller and Murmurly acts as its processor. This processing is governed by our agreement with that organisation, including the applicable Data Processing Addendum.

If your personal data is held in a customer’s workspace, the customer generally decides why it is processed and how long it is kept. The section on Customer workspace data explains what this means for you.

Your Murmurly account exists independently of any individual workspace. Account-level personal data is therefore processed separately from data held inside customer workspaces.

Murmurly is a business service and is not directed at children.

2. Website and enquiries

When you visit murmurly.io, contact us or request a demo, we may process the personal data you provide to us, such as your name, email address, organisation and the content of your message. We use this information to respond to your enquiry, arrange or follow up on a demo, and manage our business relationship.

We may also receive business contact information, such as your name, role, organisation and business contact details, from other sources, including referrals, colleagues or other business contacts, and publicly available professional or corporate sources. We use this information for sales, business development and relationship management. We rely on our legitimate interests in developing and managing business relationships (Art. 6(1)(f)).

Where permitted by applicable electronic marketing laws, we may also send business contacts information about Murmurly, product updates or related services. For the processing of personal data for direct marketing, we rely on our legitimate interests where permitted, or on consent where required. You can object to or opt out of direct marketing at any time, after which we will stop using your personal data for that purpose.

We generally rely on our legitimate interests in responding to business enquiries and developing customer relationships (Art. 6(1)(f)). If you personally enter into a contract with us, or ask us to take steps before doing so, we may rely on Art. 6(1)(b) where the processing is necessary for that purpose.

If you use Murble on our website, we process the messages you send, Murble's replies and a temporary browser identifier so that the conversation can function and we can apply reasonable usage limits. We rely on our legitimate interests in answering your request and protecting the service against misuse (Art. 6(1)(f)). The conversation is processed using Google's AI services, as described in the section on AI features. Please do not submit confidential or special-category personal data through the public website assistant.

We also use limited analytics to understand how our website performs and how its main features are used. These analytics use a pseudonymous first-party analytics cookie containing a browser identifier that expires after no more than 30 days and is not linked to your name or email address. We do not use session replay, heatmaps or automatic event capture, and we do not retain your IP address for analytics. Where geographic information is derived from your connection, we retain only city and country and discard the IP address.

We rely on our legitimate interests in maintaining and improving the website for this limited analytics processing (Art. 6(1)(f)). We configure the analytics to minimise its impact on your privacy. You can object to this limited analytics processing at any time through our Analytics preferences.

3. Your Murmurly account and use of the platform

When you create or use a Murmurly account, or otherwise interact with the Murmurly platform, we may process the account- and platform-level personal data described below independently from personal data held in a customer workspace.

We process	Why	Legal basis (GDPR)
Account and sign-in data , such as your name, email address, authentication method, authentication credentials or tokens, and information received from your chosen sign-in provider	To create your account, authenticate you and provide access to Murmurly	Performance of the User Terms, Art. 6(1)(b)
Session and security data , such as session identifiers, browser information, sign-in and security events, and audit records	To keep you signed in, secure accounts and investigate suspected misuse or security incidents	Performance of the User Terms and our legitimate interests in security, Art. 6(1)(b) for session functionality; Art. 6(1)(f) for account security and misuse prevention
Profile and preference data , such as how you want to be addressed, country, timezone, locale, stated role, AI experience settings and other account preferences	To personalise your account and provide a consistent experience across workspaces	Our legitimate interests in providing a personalised and consistent user experience, Art. 6(1)(f)
Your profile image , whether uploaded by you or received through your chosen sign-in provider	To display your account identity within Murmurly	Our legitimate interests in providing recognisable user profiles, Art. 6(1)(f)
Legal acceptance and acknowledgement records , including your account identifier, relevant workspace identifier, timestamp, document and version, acceptance or acknowledgement event and IP address	To record which User Terms or demo terms you accepted and which Privacy Policy version you acknowledged, and to maintain evidence of that record	Our legitimate interests in evidencing agreements and compliance, Art. 6(1)(f)
Support correspondence and diagnostic information	To answer support requests and investigate technical or account issues	Performance of the User Terms where necessary and our legitimate interests in providing support, Art. 6(1)(b) where support is necessary to provide the service under the User Terms; Art. 6(1)(f) for troubleshooting and service administration
Limited product analytics, including pseudonymous browser or account identifiers, workspace identifiers, coarse city and country, and a fixed set of product and technical usage events	To monitor reliability, understand aggregate use and improve Murmurly	Our legitimate interests in operating and improving the service, Art. 6(1)(f)

Certain account and authentication information is required to create and secure your account. If you do not provide this information, we may not be able to create your account or provide access to Murmurly. Optional profile information and personalisation settings may be left blank or changed by you.

If you sign a commercial agreement on behalf of an organisation, we also process your name, title, email address and the executed agreement so that we can administer and evidence our relationship with that organisation. We rely on our legitimate interests in entering into and managing business relationships (Art. 6(1)(f)).

For product analytics, we do not link the browser identifier to your name or email address. The identifier is first-party, expires after no more than 30 days and is reset when you sign out. We do not use session replay, heatmaps or automatic event capture. We do not store your IP address as part of your product session; where it is used to derive geographic information, only city and country are retained.

4. AI features

Murmurly includes AI-assisted features, including Murble, summarisation, content and template generation, information extraction, semantic search and real-time voice.

We use Google AI services to provide these features. For text-based AI features, prompts and the relevant context needed to perform your request may be processed by Google. For real-time voice, audio is streamed from your browser to Google so that the conversation can take place.

Where AI features process personal data held in a customer workspace, the customer generally remains the controller and Murmurly processes that data on its behalf. The customer controls whether and how those AI features are used within its workspace.

Murmurly does not use AI to infer, score or classify a person's emotional or psychological state, and does not create voiceprints or biometric templates. Account-level preferences such as your stated AI experience level may be used to adapt how Murble communicates with you, as described in Section 3.

We do not use personal data to make solely automated decisions that produce legal or similarly significant effects for you.

We configure our AI services so that customer data is not used to train or improve general-purpose AI models where supported by the applicable service. More information about our providers and international data transfers is provided below.

5. Customer workspace data

When a customer uses Murmurly to process personal data for its own business purposes, the customer generally acts as controller and Murmurly acts as its processor under the applicable Data Processing Addendum.

This may include information about people, organisations, engagements, events, invitations, RSVPs, notes, tasks, agendas, feedback, files and other information added to or generated within a customer workspace.

The customer determines why this personal data is processed and, subject to applicable law and its agreement with Murmurly, how long it is kept. If you want to access, correct, delete, restrict or obtain a copy of personal data held about you in a customer workspace, you should normally contact the organisation that collected or provided it. If you contact us instead, we will help direct the request to the relevant customer and provide the assistance required of us as processor.

Murmurly does not require customers to enter special-category personal data. If a customer chooses to process such data in Murmurly, the customer is responsible for ensuring that it has an appropriate legal basis and complies with the additional requirements that apply.

Google Calendar integration

Google Calendar is an optional integration that must first be enabled for the relevant Workspace by an authorised Workspace administrator. Once enabled, an individual Member may choose whether to connect their own Google Calendar account to Murmurly. Murmurly accesses Google Calendar data only after the Member initiates the connection and grants the requested Google permissions.

Murmurly provides two levels of Google Calendar functionality.

Availability

When calendar availability is enabled, Murmurly accesses the Member's calendar list and free/busy information. Murmurly stores only the start and end times of busy periods for a limited rolling scheduling period and refreshes this information when calendar availability is synchronised. Event titles, attendees, locations and event identifiers are not accessed through this functionality. The Member can see their own availability information. Other authorised Workspace users may only be shown a count of scheduling conflicts and are not shown the underlying times or the calendar from which they originate.

Personal calendar events

A Member may additionally enable access to their personal calendar events. When enabled, Murmurly may access the event title, start and end time, location, calendar name, event identifier and a link to the corresponding Google Calendar event. This information is retrieved when the Member uses the relevant functionality and is retained only temporarily, typically for approximately three minutes, as a technical cache. It is visible only to the Member whose Google Calendar account is connected. Murmurly does not retrieve attendees, event descriptions or conference links through this functionality.

To operate the connection, Murmurly also stores the Member's calendar-selection settings, connection and synchronisation status, information about the calendars available through the connected account, and the authorisation credentials necessary to maintain the

connection.

Google Calendar data is used only to provide the calendar and scheduling functionality enabled by the Customer and requested by the Member. Where this data is processed in connection with a Customer Workspace, the Customer generally acts as controller and Murmurly acts as processor in accordance with the applicable Data Processing Addendum.

Murmurly does not sell Google Calendar data, use it for advertising, or use it to train or improve general-purpose artificial intelligence or machine-learning models.

When a Member disconnects Google Calendar, disables calendar synchronisation, leaves the relevant Workspace or deletes their Murmurly account, Murmurly deletes the data associated with the Google Calendar connection from its active systems and revokes the corresponding access with Google. Deleted data may remain in backups maintained by Murmurly's hosting provider for up to 14 days before being automatically deleted.

Murmurly's use and transfer of information received from Google Workspace APIs will adhere to the Google User Data Policy, including the Limited Use requirements.

6. Who we share data with

We share personal data only where this is necessary to provide, secure and administer Murmurly, to comply with law, or where you or a customer has expressly authorised us to do so in connection with a service, integration or other arrangement that Murmurly has agreed to support.

Depending on the processing, recipients may include:

- **hosting and infrastructure providers**, which provide our application infrastructure, storage, content delivery and email delivery;
- **AI service providers**, which process information needed to provide Murmurly's AI features;
- **analytics and error-monitoring providers**, which help us understand product performance and reliability;
- **business service providers**, such as email, document storage, electronic-signature, development and support tools used for our operations;
- **authentication and identity providers**, where you choose to use a supported third-party sign-in method;
- **parties and advisers involved in a merger, acquisition, financing, reorganisation or sale of all or part of our business**, where necessary and subject to appropriate confidentiality safeguards;
- **professional advisers**, such as accountants, legal advisers and auditors; and

- **public authorities**, where disclosure is required by law.

Where a service provider processes customer workspace data on our behalf, it acts as a subprocessor under our Data Processing Addendum. Our current Subprocessor List is available at murmurly.io/subprocessors.

If you or a customer enables an optional third-party integration, API connection or other connected service made available or supported by Murmurly from time to time, personal data may be exchanged with the relevant provider or system to the extent necessary to provide that functionality. The customer controls whether such connections are enabled and can disconnect them where supported.

7. International transfers

Murmurly uses EU-based processing where this is available and appropriate for the relevant service and deployment. Personal data may nevertheless be processed outside the European Economic Area where this is necessary to provide or support Murmurly.

Where personal data is transferred to a country outside the EEA, we use an appropriate transfer mechanism as required by applicable data protection law. This may include an adequacy decision adopted by the European Commission or the European Commission's Standard Contractual Clauses, together with additional safeguards where required.

You can contact us at legal@murmurly.io if you would like information about the safeguards that apply to a particular transfer.

8. Retention and security

We keep personal data only for as long as necessary for the purpose for which it was collected, or for as long as we are required or permitted to retain it for legal, security or evidentiary purposes.

Retention periods depend on the type of data. For example:

- active account sessions are retained for up to 30 days, and expired or revoked sessions for a further 7 days;
- one-time sign-in and verification records are deleted after they expire;
- pseudonymous browser identifiers used for analytics expire after no more than 30 days, and associated browser analytics profiles are deleted after 30 days without a relevant event;
- product and website analytics events are retained for up to one year;
- account-level personal data is deleted when an account is deleted, except where specific records must be retained for another lawful purpose;

- website enquiries and business correspondence are retained while relevant to the enquiry or business relationship and are periodically reviewed;
- legal acceptance records, contracts and compliance records may be retained for the applicable legal and limitation periods; and
- accounting and tax records are retained for the period required by law.

Where Murmurly processes personal data on behalf of a customer, retention and deletion are governed by the customer's instructions and the applicable agreement and Data Processing Addendum. Following termination, customer workspace data is handled in accordance with the applicable contractual retention and deletion arrangements.

We use technical and organisational measures designed to protect personal data against unauthorised access, loss, misuse, alteration or disclosure. These measures include encryption in transit and at rest, access controls, authentication and workspace-isolation controls, logging and monitoring, backups, and incident-response procedures.

No security measure can eliminate all risk, but we review and update our safeguards as our services and risks evolve.

9. Your rights

Depending on the circumstances and the privacy laws that apply to you, you may have rights in relation to your personal data. Where the GDPR applies, these may include the right to access, correct or delete your personal data, restrict or object to its processing, and receive certain personal data in a portable format. Where processing is based on consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn.

Where applicable, you may have the right to object to processing based on our legitimate interests. If you exercise that right, we will stop the processing unless we have compelling legitimate grounds to continue or the processing is necessary for the establishment, exercise or defence of legal claims. Where the GDPR applies and we process personal data for direct marketing, you have the right to object to that processing at any time. If you do, we will stop processing your personal data for direct marketing purposes.

Where other applicable privacy laws grant you additional rights, we will honour those rights to the extent required by law.

To exercise your rights in relation to personal data for which Murmurly is controller, contact legal@murmurly.io. We may ask for information necessary to verify your identity before acting on a request.

For requests under the GDPR, we will respond without undue delay and generally within one month. Where permitted by the GDPR, this period may be extended by up to two further months where a request is complex or numerous. Requests under other applicable privacy laws will be handled within the timeframes required by those laws.

If your request concerns personal data held in a customer workspace, you should normally contact the relevant customer, as that organisation generally acts as controller. If you contact us instead, we will help route the request appropriately and provide the assistance required of us as processor.

Where the GDPR applies, you also have the right to lodge a complaint with a data protection supervisory authority. In the Netherlands, this is the Autoriteit Persoonsgegevens. You may also contact the supervisory authority in the EEA country where you live, work or believe an infringement has occurred.

10. Changes and contact

We may update this Privacy Policy from time to time to reflect changes to Murmurly, our processing practices or applicable law. The version and effective date at the top of this Privacy Policy identify the version currently in effect. Previous versions of this Privacy Policy are available on request at legal@murmurly.io.

Where a change materially affects how we process personal data, we will take reasonable steps to bring it to your attention. Where appropriate, we may ask account users to acknowledge an updated version of this Privacy Policy.

If you have questions about this Privacy Policy or our processing of personal data, or if you want to exercise your privacy rights, you can contact us at:

Murmurly B.V. Alkmaar, the Netherlands Chamber of Commerce (KVK): 42165731
legal@murmurly.io