Accorded Privacy Policy

Effective date: 2 November 2026

This Privacy Policy explains how Accorded collects, uses, shares, stores, and protects personal information when people visit the Accorded website, use the Accorded application or browser extension, join a waiting list, submit questions, or use related services.

1. Information Accorded May Collect

Depending on how the service is used, Accorded may collect:

- Account details such as name, email address, organisation, preferences, and authentication information.

- Contact and support information submitted through forms or support channels.

- Website information such as pages viewed, browser and device information, approximate location derived from IP address, cookies, session activity, and diagnostic information.

- Application and extension information such as version, settings, workflow activity, performance information, and error reports.

- LinkedIn and professional information accessed or supplied by an authorised user, including profile content, posts, comments, role history, and public professional language.

- User content such as messages, email conversations, meeting notes, transcripts, drafts, chat questions, files, and relationship context.

- Assessment information such as pattern results, confidence information, active assessments, history, and saved contact information.

- Marketing information such as campaign settings, imported contact details, delivery status, and subscriber-group status when an administrator uses the marketing workflow.

- Transaction and subscription information. Payment card information may be handled directly by a payment provider rather than stored by Accorded.

- Account setup, invitation, email-verification and security records; verification status and deadlines; subscription phase, free-term start/expiry and notification records; and safe operational activity counts.

2. How Accorded Collects Information

Accorded may collect information directly from users, automatically through the website or extension, or from third-party services that users choose to connect. The extension only supports workflows initiated by the user and is not intended to collect unrelated browsing activity.

3. How Accorded Uses Information

Accorded may use information to:

- Provide, operate, maintain, and improve the service.

- Assess professional and written communication patterns.

- Translate and help draft messages.

- Maintain saved contacts and communication history.

- Provide shared team workspaces where authorised.

- Generate assessment views and PDF reports.

- Provide the optional marketing workflow where an administrator authorises it.

- Process support requests and communicate about the service.

- Secure the service, diagnose failures, prevent misuse, and comply with legal obligations.

- Analyse submitted website questions and improve help content, where permitted.

- Complete signup and invitations, verify addresses, protect account access, apply plan allowances and fixed-term expiry, and send setup, security, billing and free-access notifications.

4. Ask Accorded Questions

Ask Accorded is available on the website and in Customer Hub help, onboarding and contact guidance. A question may be sent to a configured AI service provider so that the service can construct an answer using Accorded's approved FAQ, features-and-benefits, privacy, and terms content.

Submitted questions may be stored with the time submitted, the knowledge content used to answer them, the answer status, and a version of the published content. This information may be used to identify unclear pages and improve the service.

Before a question is classified, sent to an AI provider or recorded, Accorded checks for detected sensitive values and replaces their non-whitespace characters with dashes. The question textarea is updated so the user can see the replacements. Detected values may include credentials, card or bank identifiers, email addresses and phone numbers. For authenticated help, known relevant account contact details and the licence key may also be masked. Only the sanitised question is used in the help request and stored question record; the original values are not retained in that record or ordinary diagnostics. General questions mentioning passwords, cards or subscription cancellation are not blocked merely for mentioning those topics.

Visitors should not include confidential business information, passwords, credentials, sensitive personal information, or private third-party information in a website question.

Redaction is a protective measure, not a guarantee that all sensitive information will be detected. Review the updated question and avoid supplying secrets.

AI-generated answers may be incomplete or incorrect. The published Accorded pages, this Privacy Policy, and the formal Terms and Conditions take precedence over an AI-generated response.

5. AI Service Providers

Accorded may use configured third-party AI providers to process information needed for assessments, communication assistance, message drafting, or website question answering. The providers used may vary by account configuration and feature. Provider privacy terms, processing locations, retention practices, and contractual commitments also apply.

Accorded does not represent that an AI provider will retain or use information in a particular way unless that position is confirmed by the applicable provider agreement and service configuration.

When Contact Chat uses earlier correspondence, bounded context from relevant saved Comms Profile communications, account-shared emails and the requesting user's own private emails may be provided to the selected AI provider alongside the current Chat and pasted material. Other users' private emails are excluded. Long communications and the combined context are bounded, so not every record or its

full text is included. Saved Chat History records are not automatically added as this context. Saving or sharing generated material can disclose its contents to account colleagues; review it first. Only submit material you are authorised to use.

6. Sharing Information

Accorded may share information with service providers that host infrastructure, process AI requests, deliver email, manage waiting lists, support security, process payments, provide analytics, or otherwise operate the service. Accorded may also share information when directed by the user, required by law, needed to protect rights and safety, or involved in a business transfer.

For the waiting list and marketing workflow, Accorded may use Sender.net and other configured delivery services. Their own terms and privacy policies also apply.

7. Team Workspaces

When Accorded is used in a team workspace, saved contacts, assessments, communication context, and related information may be visible to authorised members of that workspace. Users should only upload information they are authorised to share with the workspace.

8. Referral Invitations

A customer may voluntarily submit a referee's name, optional company name, and email address in the Customer Hub Referral Link section. Accorded retains these details as a referral-invitation record for referral administration and future follow-up.

If the customer chooses Invite by email, Accorded sends the supplied email address and invitation content through the configured email provider. If the customer chooses Invite by link, Accorded stores the submitted details but does not send an email, then displays the referral URL for the customer to share. Referral URLs contain attribution information.

Referral details are protected by customer access controls, are not public, and are not used as contact-assessment content, Contact Chat context, or general marketing content unless separately authorised. Users should only submit details they are permitted to share. A referee who was not expecting an invitation can ignore it. Existing retention, deletion, processor, and privacy-request processes apply.

9. Legal Bases Where Required

Where applicable law requires a legal basis, Accorded may rely on consent, performance of a contract, legitimate interests, legal obligations, or another permitted basis. The relevant basis may depend on the feature and the user's relationship with Accorded.

10. Cookies And Similar Technologies

Accorded may use cookies, local storage, analytics tools, pixels, and similar technologies to maintain sessions, remember preferences, understand usage, measure performance, and protect the service. Blocking some technologies may affect functionality.

If a user chooses Remember this browser during two-factor sign-in, a security cookie recognises that browser for up to 30 days. Ordinary logout does not remove that trust; the user can revoke remembered browsers from Login details. Account setup and verification links use limited-purpose access controls and are not a substitute for normal sign-in.

Accorded video pages embed YouTube using its privacy-enhanced player and do not autoplay. Loading the embedded player may still disclose browser, device and network information to YouTube; playing a video may involve further processing under Google's privacy practices. The player is a third-party

service, not an Accorded-hosted video file.

11. International Processing

Information may be transferred to, stored in, or processed in countries outside the country where the user lives. Where required, Accorded uses appropriate safeguards for cross-border transfers.

12. Retention

Accorded keeps information for as long as reasonably necessary to provide the service, maintain accounts, preserve assessment and delivery records, meet legal obligations, resolve disputes, protect security, and support legitimate business needs. Retention varies by information type, feature, account status, legal requirement, and user request.

Expiry of a fixed-term free plan or a restriction for overdue email verification does not itself delete saved contacts, assessments, chats or communications. Existing records remain available through permitted account access, subject to separate restrictions and these retention criteria. Expiry does not promise indefinite retention. Users may request access, download or deletion through the existing account and privacy-request processes.

13. User Choices And Rights

Depending on location, users may have rights to access, correct, delete, download, restrict, or object to certain processing. Users may also unsubscribe from marketing messages. Requests can be sent to translate@accorded.co.uk; Accorded may need to verify identity before responding.

14. Security

Accorded uses administrative, technical, and organisational measures designed to protect information. No service or transmission can be guaranteed to be completely secure. Users are responsible for protecting their credentials and devices.

Optional authenticator-app two-factor authentication uses protected setup information, encrypted authenticator secrets, hashed single-use recovery codes, limited login challenges and security-event records. It protects normal Customer Hub sign-in, not separate extension licence/email or API/MCP credential paths. Users should secure those credentials independently and never share authenticator or recovery codes in help questions.

Accorded records email-verification status and limited-purpose link information to verify addresses and recover setup. A new-signup verification deadline may restrict product use but does not stop billing or delete data. For verified accounts, a new login email is applied after confirmation; correction of a newly registered unverified address takes effect after the required security checks and preserves the original deadline. Security notifications and service emails are distinct from optional marketing communications.

15. Children

The service is not intended for children under 13. Accorded does not knowingly collect personal information from children under 13 and will take appropriate steps when notified of such information.

16. Changes And Contact

Accorded may update this Policy and will update the effective date. Privacy questions and requests can be sent to translate@accorded.co.uk.

This document should receive legal review before being treated as jurisdiction-specific legal advice or a complete statutory privacy notice.

17. Connected Workspace Data And Choices

When a user chooses to connect a workspace, Accorded processes the access and refresh tokens, provider identifiers, selected calendar or task list, synchronisation preferences, linked item fields and limited change history needed for that feature. Tokens are encrypted. Calendar and task synchronisation reads or writes supported fields of Accorded-linked items. An appointment availability check reads busy periods in the selected calendar, not unrelated appointment descriptions. It does not import the user's entire calendar. A separate optional agenda is distinct from the private Pre-call Briefing.

Read-only mailbox logging requires a separate connection and permission. It processes message identifiers, dates, sender and recipient addresses, subjects and bounded message text to associate correspondence with saved contact email addresses. Attachments are not imported. An ambiguous address is not assigned by guessing a person's identity. A user chooses whether new eligible correspondence is shared with their account team or kept only for themselves. Any account user can make a contact's mailbox correspondence private across the account; only that user or a Customer Admin can make the contact public again. This does not hide the contact card. Each user's private inbound and outbound emails remain accessible only to that user, including when another user set the privacy rule. The mailbox owner can explicitly share individual messages. Making a contact public does not expose earlier unshared private emails. A mailbox connection does not itself authorise sending, modifying or deleting provider messages. Account administrators and ordinary support access do not automatically gain access to private imported message bodies.

Comms reassessment can use Saved Messages, Synced Emails or both, with at most 15 eligible communications combined. Each run that includes synced emails requires confirmation that eligible contact-authored emails from the requesting user's mailbox and account-shared emails from other mailboxes may be sent to the displayed AI provider at the displayed credit quote. Approval also covers saving the generated assessment on the shared contact, where account colleagues can see it and it may become active under the usual rules. Original private emails remain private; the approved derived assessment is not a private result. Other users' private emails are excluded. Outgoing messages, signatures and quoted thread history are not treated as the contact's original language; attribution and quote removal have limitations requiring human review. Automated mailbox reassessments are not enabled. Notifications can tell the user when enough new evidence is available; users can turn these off or set per-contact pauses, including never reminding again. An alert does not run an assessment or authorise charges. Assessments are probabilistic communication guidance, not facts about personality, a diagnosis or an instruction to make solely automated consequential decisions.

When a user requests communication drafting in Contact Chat, relevant bounded context may include account-shared emails and that user's own private emails. Another user's private emails are not supplied. Chat uses the selected configured AI service. Saving or deliberately sharing generated material can disclose its contents to account colleagues; users should review it for private information first. Existing deliberately saved reports, chats and exports are separate historical records, not live access to a mailbox.

Imported mailbox records use the user's available retention choice, normally 90 days and no more than 365 days in this feature. Selected email text is encrypted separately while a Comms assessment runs; those working copies are removed on completion or source deletion. Expiry and deletion remove imported messages and legacy private email-assessment copies through bounded maintenance. Shortening retention immediately excludes older source messages from new use while deletion completes. Disconnecting removes the saved connection credentials and stops new synchronisation; it is separate from deleting already imported records. Completed shared assessments, saved Chats and records deliberately shared or exported have their own retention and deletion requirements; source

deletion does not silently erase them. Users should review those records when requesting erasure. Service notifications are not marketing subscriptions.

The customer normally determines why its business contact information and correspondence are processed; Accorded processes it to provide the configured service under the applicable contractual arrangements. Accorded remains responsible for its own account, security and service administration purposes. A user's OAuth consent is not, by itself, a lawful basis for every use of other people's correspondence. Customers must consider transparency, necessity, minimisation, rights requests and international transfers. Provider permissions and organisational policies may impose additional limits.

Use and transfer of information received from Google APIs must comply with the Google API Services User Data Policy and its Limited Use requirements. Connected workspace information is not used for advertising, sold, used to train general-purpose models or pooled across customers for unrelated purposes. Human access is restricted to the limited circumstances allowed by the applicable provider policy and law. Provider verification, security assessment and legal review may be required before public availability; this policy does not claim that any certification or approval has been obtained.