

# Privacy Policy

How Heyou treats personal data — including the two-tier model that separates organizational data from individual users' personal-tier connections, and what we do not do with either.

Version 1.9

Effective 23 October 2026

Last updated 25 October 2026

[heyou.io/privacy-policy/](https://heyou.io/privacy-policy/)

## 1. Our Role and How We Organize Data

Heyou is a relationship intelligence platform that helps organizations and their users map existing professional networks and surface relevant relationship paths within them. We organize the data we process into two distinct tiers, each with its own access rules and legal treatment.

### The Two-Tier Data Model

**Organizational tier (Customer Data).** Data the organization connects or that Users contribute in the course of their work for the organization. This includes CRM records, corporate email and calendar metadata, employee directory information, and professional network data — professional connections, public posts, and public profile fields that a User is exposed to through the User's authenticated session on professional platforms, contributed to the organization's relationship graph as part of the User's work. Organizational-tier data is available across the Customer's tenant subject to the Customer's internal permission model. The Customer is the Controller for this data; Heyou is the Processor.

**Personal tier (User Data).** Data an individual Authorized User chooses to connect from intrinsically personal resources they control — a private email account, a personal messaging app, or direct private one-to-one messages on a professional network visible only to that User. User Data is held at the User level within the tenant. It is not visible to the Customer, Customer admins, or other Authorized Users unless the User affirmatively chooses to share specific data with the organization. The User is the Controller for User Data; Heyou processes it on the User's behalf per the User's acknowledgment at connection time.

### Where Relationship Information Comes From

Heyou builds relationship information from sources including business systems an organization connects, sources an individual user authorizes (read within that user's own access), and information users provide when using Heyou. From these, Heyou derives relationship insights, such as how strong a relationship appears to be.

### What Heyou Processes and What Heyou Does Not Process

Heyou processes only what is necessary to map relationships and surface recommendations. For personal messages connected at the User tier, Heyou never ingests, stores, or processes the content of those messages — only metadata such as from, to, timestamp, interaction frequency, and similar non-content signals used to infer relationship strength. Heyou does not read the substance of any personal communication between a User

and another person. Questions a User addresses to Heyou through a messaging channel are covered separately in Section 5.

## What Heyou Does Not Do

Heyou is not a data broker. Heyou does not operate, sell, or license a contact database. Heyou does not collect data for a Heyou-owned directory or data product. Customer Data is held in the Customer's logically isolated tenant; User Data is held at the User level. Data is not used outside the context of the relevant tenant for cross-customer use cases.

Heyou does not aggregate Personal Data across customers to build any marketable directory or people-search product. Heyou does not operate a general-purpose public web crawler and is not designed to bulk-harvest external platforms. Where Heyou reads professional context from user-authorized sources, processing is scoped to the authorized user context, customer configuration, and applicable product controls. When Heyou presents an email address or phone number, it comes only from Customer Data, such as organizational systems or professional network data Users contributed to the organization, or from User Data, such as personal resources a User connected. Heyou does not use third-party enrichment, data-broker sources, or public scraping to obtain or supplement contact details.

Heyou does not use Customer Data or User Data to train third-party generative AI foundation models. Heyou may use Customer Data, User Data, and signals derived from them to improve its own proprietary non-generative relationship-scoring, classification, calibration, and path-ranking models as part of delivering and enhancing the Services, subject to the DPA, applicable agreement, user acknowledgment where applicable, tenant-isolation safeguards, cross-tenant leakage safeguards, and any applicable Order Form restrictions.

## Connected CRM Systems

Where a Customer connects a CRM such as Salesforce or HubSpot, Heyou reads account, opportunity, opportunity-contact-role, contact, lead, user, activity, and contract records to improve recommendation relevance and measure outcomes.

Heyou stores a narrowed projection of those records rather than a copy of the CRM. It keeps identifiers, ownership, stage and lifecycle values, and timestamps. It does not store CRM display data or contact details: email addresses are not stored in readable form, and activity records are reduced to who, what type, and when, with no field for a subject line or body.

Where the Customer enables it, Heyou writes its own recommendations and their status back into records Heyou installs in the Customer's CRM under a dedicated namespace. Heyou writes nothing to the Customer's standard CRM objects and holds no delete rights on them; records in Heyou's own namespace are purged by the installed Heyou package inside the Customer's CRM on the window the Customer configures. This connection is Customer-authorized at the organizational level and is organizational-tier Customer Data under the model above.

## User-Identified Targets Not in Connected Systems

A User may identify individuals as targets for outreach who do not appear in the Customer's CRM or other connected systems. For these individuals, Heyou processes only the minimum information needed to surface a relationship-path recommendation, drawing on information that is publicly available or accessible through the User's authorized sources. Heyou does not store these individuals' email addresses unless those addresses are already present in Customer Data or User Data, does not send them messages, and does not contact them on

the Customer's behalf. Heyou's outputs are recommendations; any outreach is initiated by the User through the User's own channels.

## Roles Under Data-Protection Law

For Customer Data, including professional network data contributed by Users in the course of their work, the Customer is the Controller and Heyou is the Processor. Processing is governed by the DPA.

For User Data, unless otherwise agreed in writing with the Customer, the individual Authorized User controls the connection, visibility, and sharing of that User Data, and Heyou processes it on the User's behalf under the User's acknowledgment at connection time and this Privacy Policy. This user-level control model does not make User Data visible to the Customer, Customer admins, or other Authorized Users unless the User affirmatively shares specific data with the organization.

For website visitors, prospects, and individual account sign-ups on Heyou properties, Heyou acts as the Controller. This Privacy Policy describes that Controller processing.

## 2. Personal Data We Collect in Our Controller Role

Heyou may collect the following Personal Data where it acts as Controller:

- **Account and contact data:** name, business email, employer, job title, phone, and information provided in forms, demo requests, or support interactions.
- **Communications:** emails, chats, support requests, and call recordings or meeting notes with sales, success, and support teams where used.
- **Marketing data:** interactions with emails, events, webinars, and ads; preferences; and unsubscribe status.

## 3. How We Use Personal Data and Legal Bases

| Purpose                                                | Legal basis under GDPR where applicable                |
|--------------------------------------------------------|--------------------------------------------------------|
| Providing Heyou properties and evaluating the platform | Contract; legitimate interests                         |
| Responding to inquiries and support                    | Contract; legitimate interests                         |
| Sending marketing communications                       | Consent where required; legitimate interests otherwise |
| Product analytics and improvement                      | Legitimate interests                                   |
| Security, fraud prevention, and abuse detection        | Legitimate interests; legal obligation                 |
| Complying with law and responding to legal process     | Legal obligation                                       |
| Corporate transactions                                 | Legitimate interests                                   |

## 4. Google Workspace Integrations

An Authorized User may connect their Google Calendar to Heyou. This section describes that integration specifically. Where anything in this section conflicts with another provision of this Privacy Policy, this section controls for data Heyou receives from Google APIs.

## Limited Use

Heyou's use and transfer of information received from Google APIs to any other app will adhere to the [Google API Services User Data Policy](#), including the Limited Use requirements.

## Scope Requested

Heyou requests read-only access to the User's Google Calendar events, and only the narrowest scope that supports the features described below. Heyou does not request write access, and does not create, edit, or delete calendar data. Google presents the specific permissions requested at the point of consent, and a User can review or revoke them at any time through their [Google Account permissions page](#). If Heyou later introduces a feature requiring different access, Heyou will request it separately and update this policy.

## What Heyou Reads and Why

With the User's consent, Heyou reads the User's own calendar events for two purposes, both shown to the User in the Heyou app:

- **Finding introduction paths.** Heyou identifies the people the User has met and how recently, to help the User find relevant introduction paths.
- **Identifying meetings booked from Heyou recommendations.** Where the Customer's order with Heyou charges per booked meeting, Heyou identifies meetings booked with people it recommended, and the first meeting booked at an account it recommended a path into, shows them to the User and the Customer, and counts them under that order. The charge record holds a recommendation identifier, the account, the dates and the rate tier, and no individual's identity. Where the Customer connects company calendars on another provider the Services support, such as Microsoft 365, Heyou reads the same data for the same purposes and applies the same retention. Heyou does this only for company calendars administered by the Customer, on Google Workspace or another provider the Services support, never for calendars on personal accounts.

For these purposes Heyou uses:

- **Attendee email addresses, attendee display names, meeting times, and the date each event was created,** to establish who the User has met and when, and when a meeting with a recommended person, or the first meeting at a recommended account, was booked.
- **Event title, description, location, and conferencing details,** to distinguish real meetings from all-day blocks, out-of-office entries, and room-only holds, which would otherwise be recorded as relationships that do not exist.

Heyou uses this data to provide and improve the user-facing features described above, and for no unrelated purpose.

## Tier, Visibility, and Access

Which tier a connected Google Calendar falls into under the two-tier model in Section 1 depends on the Google account it belongs to:

- **A calendar on a personal Google account** the User controls is personal-tier User Data. It is held at the User level, and is not visible to the Customer, Customer admins, or other Authorized Users unless the User affirmatively chooses to share specific data with the organization.
-

**A calendar on a Google Workspace account administered by the Customer** is corporate calendar data and is organizational-tier Customer Data, consistent with Section 1. The Customer is the Controller, and the DPA governs that processing.

The Google Limited Use commitments in this section — including the scope, personnel-access, AI and machine-learning, retention, and transfer commitments — apply to data Heyou receives from Google APIs regardless of which tier it falls into.

Heyou does not allow its personnel to read Google user data, except: with the User's affirmative agreement to view specific data, including where the User requests support and access is necessary to provide it; where necessary for security purposes such as investigating abuse or a suspected incident; to comply with applicable law; or where the data has been aggregated and anonymized for internal operations; or, at the Customer's request, to verify a charge the Customer disputes under the Terms of Service, limited to the booking date, the meeting date, and whether a recommended person was on the invite.

## AI and Machine Learning

Heyou does not use Google user data to develop, improve, or train generalized or non-personalized AI or machine-learning models. Any learning derived from it stays within the personalized experience of the User from whose account it was authorized.

## Retention and Deletion

Calendar-derived signals are retained for as long as the User keeps the integration connected and their account active, and are handled under our [Data Retention and Deletion Schedule](#). A User may disconnect the integration at any time from within Heyou, and may revoke Heyou's access directly through their [Google Account permissions page](#). For a calendar on a personal Google account, Heyou deletes the calendar-derived data associated with that User from production systems within 30 days of disconnection or account deletion. For a calendar on a Customer-administered account, that data is Customer Data and follows the Data Retention and Deletion Schedule. In both cases, records of meetings already counted under the Customer's order, which hold a recommendation identifier, the account and dates and no individual's identity, are kept as billing records as set out in that schedule. Residual copies in backups expire within 30 days.

## Transfer and Sale

Heyou does not transfer or sell Google user data to third parties such as advertising platforms, data brokers, or information resellers, and does not use it for serving advertisements, including retargeting, personalized, or interest-based advertising. Heyou does not use Google user data to determine creditworthiness or for lending purposes.

## 5. Query Channels (Slack, WhatsApp, and Claude)

An Authorized User may ask Heyou questions from Slack, WhatsApp, or Claude instead of the Heyou web application. Each of these is a query surface: the User asks a question, and Heyou answers from data that User is already authorized to see. All three reach Heyou through the same interface, and the commitments in this section apply to all of them.

## What Heyou Reads

Heyou reads the question the User sends it, and the identifier needed to authenticate the User and route the answer back — the Slack user and workspace identifiers, the WhatsApp phone number the User messages from, or the account identifier established when the User connects the Claude connector. Heyou uses these only to authenticate the User against their Heyou account, answer the question, and reply. Heyou reads only what the User sends it, and takes nothing further from the surrounding conversation.

## What Heyou Does Not Read

Heyou does not read Slack channels, direct messages between other people, message history, files, or workspace membership; does not read a User's WhatsApp conversations with anyone other than Heyou; and does not read a User's Claude chat history, memory, projects, or any conversation content beyond the question put to Heyou. On every channel, Heyou does not build a relationship graph, index, or other lasting store from what it reads, other than corrections a User asks Heyou to record, and does not use it to train any large language model. Nothing a User sends through these channels is used to generate answers for any other organization or User.

## What the Channels Can Do

These channels are for asking Heyou questions. A User cannot use them to send a message, post, or take any externally visible action, and cannot use them to change data in a connected third-party system. A User can ask Heyou to record a correction to a relationship, with a reason. Corrections are Customer Data, visible within the organization under its permission model, and kept until removed. Answers are information the User could already retrieve in the Heyou app.

## Questions and Answers

Heyou treats all three channels the same way. A question sent to Heyou, and the answer Heyou returns, are retained only as long as needed to operate the conversation the User is having, and are then deleted. Heyou does not archive or index them, does not use them to build any relationship graph or other lasting store, and does not use them to train any large language model.

A question may arrive with context, such as the User's goal or the state of a deal ("request context"). Heyou uses request context to answer the question and keeps it only for the limited period set out in the Data Retention and Deletion Schedule. Request context is not used to train generative AI models.

The identifiers that link a User to their Heyou account — the Slack user and workspace identifiers, the User's WhatsApp phone number, or the Claude connector account identifier — are kept for the life of the channel connection, because the channel cannot authenticate the User without them. They are deleted when the User disconnects the channel, the Slack app or Claude connector is uninstalled, the User requests deletion, or the account is deleted. A User can request deletion at any time by replying to the conversation or by emailing [privacy@heyoudotio](mailto:privacy@heyoudotio).

Full periods are in our [Data Retention and Deletion Schedule](#). These retention commitments cover what Heyou holds. Where a User queries Heyou from their own AI environment, that environment keeps its own record of the conversation under the User's or their organization's arrangements with that provider. These are messages the User addresses to Heyou. The commitment elsewhere in this policy that Heyou does not process the content of personal messages refers to a User's communications with other people, and is unaffected.

## Automated Responses

Answers in these channels are generated by a Heyou AI agent, not by a person. Heyou identifies itself as an automated agent in the channel. Users can reach a person through the support paths in the Contact section below.

For Slack, WhatsApp, and the Heyou app, Heyou runs the reasoning that produces an answer on its own infrastructure, using the model providers listed in our [Responsible AI Policy](#) and [Subprocessor List](#). Where a User queries Heyou from their own AI environment, such as the Heyou Claude connector, Heyou authenticates the User and returns the relationship data they are authorized to see, and the model call runs in that environment under the User's or their organization's own arrangements with its provider.

## WhatsApp Opt-In

Heyou messages a User on WhatsApp only where the User has provided their number and opted in to receive messages from Heyou, and only for the purposes the User opted in to — answering their questions and delivering notifications they have enabled. Heyou does not message anyone who has not opted in. A User can stop messages at any time by replying to that effect or by disconnecting the channel in Heyou.

## The Platforms

Slack, WhatsApp, and Claude are operated by Slack Technologies, LLC, Meta Platforms, Inc., and Anthropic, PBC respectively. Use of each platform is governed by the User's or the Customer's own relationship with that provider and by its privacy policy. Heyou's use of Slack APIs is subject to the Slack API Terms of Service, Heyou's use of the WhatsApp Business Platform is subject to Meta's applicable terms, and Heyou's connector in the Claude Connectors Directory is subject to the Anthropic Software Directory Terms and Policy. See our [Subprocessor List](#) for how each is treated.

## 6. Sharing

We share Personal Data with the following categories of recipients:

- **Service infrastructure and product delivery:** hosting and cloud infrastructure, authentication, application monitoring and logging, AI model providers, transactional messaging, and payment processing.
- **Website, marketing, and business operations:** website hosting, lead capture, scheduling, call recording and transcription for sales and customer-success conversations, internal CRM, and product analytics.
- **Professional advisors:** auditors, lawyers, accountants, and bankers under confidentiality.
- **Authorities:** where required by law and subject to our government request commitments.
- **Acquirers:** in connection with a merger, acquisition, or sale of assets, with appropriate notice where required.

We do not sell Personal Data and do not share Personal Data for cross-context behavioral advertising as those terms are defined under the CCPA/CPRA.

## 7. International Transfers

Heyou is headquartered in Israel, and Customer Data for EU tenants is primarily stored and processed in the European Union on Google Cloud infrastructure. Israel benefits from an EU adequacy decision, so transfers of Personal Data from the EEA to Heyou personnel in Israel may rely on that adequacy status.

For subprocessors located outside the EEA or outside an adequate jurisdiction, Heyou relies on appropriate transfer mechanisms such as the EU Standard Contractual Clauses, the UK International Data Transfer Addendum, the EU-US Data Privacy Framework where applicable, and transfer impact assessments where appropriate.

## 8. Retention

We retain Personal Data only as long as needed for the purposes described in this Privacy Policy, the DPA, the applicable agreement, or as required by law. The Data Retention and Deletion Schedule sets default retention periods by data category, unless overridden by customer configuration, contractual requirement, legal obligation, or documented security need.

### Disconnecting a Source

A User can disconnect an authorized source at any time, and Heyou then stops accessing it. Information from a personal source, and the insights derived from it, are deleted within the period set out in the Data Retention and Deletion Schedule, subject to backup cycles and legal requirements. Information the User contributed to their organization is Customer Data and is handled under the organization's instructions.

### Evaluation Briefs on heyou.io

If you create an Evaluation brief on heyou.io — the optional shareable AI Brief generated from the site's interactive flow — that brief and any work email you submitted for co-branding are retained for **one (1) day** from creation and then automatically deleted. You can request immediate deletion at any time before that by emailing [privacy@heyou.io](mailto:privacy@heyou.io) with the evaluation URL or brief ID; we will delete it on receipt.

## 9. Your Rights

Depending on where you live, you may have the right to access, correct, delete, port, restrict, or object to processing; to withdraw consent; and to lodge a complaint with a supervisory authority.

To exercise rights, contact [privacy@heyou.io](mailto:privacy@heyou.io). We will respond within the period required by applicable law and will not discriminate against you for exercising your rights.

### If You Are Not a Heyou User

Heyou may process professional information about prospects, contacts and other people in its customers' relationship graphs, such as name, role, employer, professional profile information, the fact and timing of professional interactions with customers' users, and insights derived from these. Generally, the customer is the controller of this information and Heyou processes it on the customer's behalf; the customer is responsible for the legal basis and for notices. You can ask to see, correct or delete the information Heyou holds about you, including inferred relationships, through the customer or by writing to [privacy@heyou.io](mailto:privacy@heyou.io); we will act on it or pass it to the relevant customer, as applicable. Where you ask us to delete your information or stop processing it, we may keep a minimal record so it is not collected again. Heyou does not disclose its proprietary methods in response to a request.

## Right to Object

Where Heyou or its Customer relies on legitimate interests to process Personal Data, data subjects may have the right to object. Where the objection relates to Personal Data Heyou processes as a Processor on behalf of a Customer, Heyou will support the Customer in assessing and responding to the request. Heyou may also maintain a suppression list for the limited purpose of preventing re-introduction of data where required to honor valid objections or opt-outs.

## 10. Children

The Services are not directed to individuals under 16, and Heyou does not knowingly process children's Personal Data as part of the standard service.

## 11. Security

We implement administrative, technical, and physical safeguards appropriate to the risk, described in the Security Overview. No system is perfectly secure. We maintain an incident response program and notify Customers of incidents affecting Customer Data in accordance with the DPA.

## 12. Government Requests

Heyou does not provide governments with direct, unfettered, or bulk access to Customer Data. We require valid legal process, challenge overbroad requests where appropriate, and, unless legally prohibited, notify affected Customers so they can seek protective orders.

## 13. Changes

We will post material changes to this Privacy Policy and provide notice where required by law or contract.

## 14. Automated Decision-Making

Heyou does not use automated processing, including profiling, to make decisions that produce legal or similarly significant effects on any individual within the meaning of GDPR Article 22 or equivalent regimes. Heyou's AI agents generate suggestions, such as relationship paths, draft messages, and relationship summaries. Heyou does not take externally visible actions through a User's connected accounts, such as sending messages, connecting, posting, commenting or reacting. Any outreach is carried out by the User. Heyou's Acceptable Use Policy prohibits Customers from using Heyou outputs to make hiring, firing, promotion, performance, compensation, credit, insurance, immigration, housing, or other high-stakes decisions about individuals.

## 15. Contact

- Data protection: [dpo@heyoudo.io](mailto:dpo@heyoudo.io)
- General privacy: [privacy@heyoudo.io](mailto:privacy@heyoudo.io)
- Security: [dpo@heyoudo.io](mailto:dpo@heyoudo.io)