

Data Processing Addendum

The data-protection addendum that governs Heyou as a processor on your behalf, including GDPR-aligned obligations and a summary of our technical and organizational measures.

Version 1.7

Effective 23 October 2026

Last updated 25 October 2026

heyou.io/dpa/

1. Scope and Roles

This DPA applies when Heyou Processes Personal Data on behalf of Customer. Customer is the Controller; Heyou is the Processor. For Personal Data of Data Subjects whose data Customer has made available to Heyou, including Customer's employees, Customer's prospects, contacts, and other individuals in Customer's relationship graph, Customer is responsible for having a valid legal basis and providing all required notices.

For the recommendation and charge records that Heyou keeps to charge meetings under an Order Form, described in the Data Retention and Deletion Schedule, Heyou is an independent controller. Charge records contain a recommendation identifier, the account's name or domain, the booking and meeting dates, and the rate tier, and no natural person's name, email, or role.

2. Processing Details

Subject Matter

Provision of the Services.

Duration

The Subscription Term and the post-termination export and deletion period, and, for recommendation and charge records only, the periods described in Section 4 of the Terms of Service.

Nature and Purpose

Mapping and scoring the relationship graph available to the Customer's organization; surfacing relationship paths; generating AI-assisted outreach recommendations; preparing relationship-action recommendations and related in-product workflows requested by Authorized Users; identifying meetings booked with people Heyou recommended, and the first meeting at an account Heyou recommended a path into, where the Order Form charges per booked meeting; improving Heyou's proprietary non-generative relationship-scoring, classification, calibration, and path-ranking models used to deliver the Services; and deriving aggregated, de-identified statistical insights used to operate, secure, and improve the Services.

Heyou does not provide Customer Data to any third-party large-language-model provider for the purpose of training that provider's foundation models. Heyou does not use one customer's business-specific relationship

graph, messaging patterns, account strategy, or outreach performance to generate business-specific recommendations for another customer, unless expressly agreed in the applicable Order Form or DPA.

3. Data Tiers and Sources

Heyou processes Personal Data across two tiers.

Organizational Tier — Customer Data

Data the Customer makes available at the organizational level, including: (a) CRM, corporate email and calendar metadata, and employee directory from Customer-authorized integrations; and (b) professional network data contributed by Authorized Users — 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. The Customer is the Controller for this tier; Heyou is the Processor and this DPA governs processing.

Personal Tier — User Data

Data that an Authorized User connects from intrinsically personal resources the User controls, such as a private email account, a personal messaging app, or direct private one-to-one messages on a professional network visible only to the User. User Data is held at the User level and is not available to the Customer, including Customer admins, or to other Authorized Users unless the User affirmatively shares it. Unless otherwise agreed in writing with the Customer, the individual Authorized User controls the connection, visibility, and sharing of User Data, and Heyou processes User Data on the User's behalf per the User's in-product acknowledgment at connection time. This DPA does not govern Heyou's processing of User Data unless otherwise agreed; the User-Heyou relationship is direct and governed by the Privacy Policy and the User's acknowledgment. Nothing in this model makes User Data visible to the Customer, Customer admins, or other Authorized Users unless the User affirmatively shares specific data with the organization. Heyou applies to User Data materially equivalent technical and organizational measures, subprocessor controls, transfer safeguards and incident procedures to those it applies to Customer Data.

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.

4. Data Minimization for Personal-Tier Sources

For personal messaging and similar resources connected as User Data, Heyou processes only metadata such as from, to, timestamp, interaction frequency, and similar non-content signals used to infer relationship strength. Heyou never ingests, stores, or processes the content of personal messages connected as User Data.

5. Categories of Data Subjects

Categories of Data Subjects include:

1. Customer's employees, contractors, and Authorized Users;
2. Customer's prospects, customers, partners, and other business contacts who appear in connected systems;
3. Third parties an Authorized User has identified as a target for outreach, even if not present in the Customer's connected systems; and

4. Other individuals whose professional information is visible to Authorized Users through their authorized sources, such as members of their extended professional network.

6. Categories of Personal Data

Categories of Personal Data may include:

- Identifiers such as name, business email, phone, and public professional profile URLs;
- Employment data such as employer, title, tenure, and organizational relationships;
- Communication metadata such as sender, recipient, and timestamp for corporate email where enabled by Customer;
- Calendar metadata such as attendees, times, and subjects where enabled by Customer;
- For a connected Google Calendar: attendee email addresses, attendee display names, meeting times, and the date each event was created, together with event title, description, location, and conferencing details used solely to distinguish real meetings from all-day blocks, out-of-office entries, and room-only holds. Where the Order Form charges per booked meeting, Heyou also uses attendee email addresses and domains, attendee roles, meeting times and event-creation dates from company calendars administered by Customer, on Google Workspace, Microsoft 365, or another provider the Services support, never from personal accounts, to identify meetings booked with people Heyou recommended and the first meeting at an account Heyou recommended a path into. The resulting charge record holds a recommendation identifier, the account, the dates and the rate tier, and no individual's identity. Where the calendar belongs to a Google Workspace account administered by Customer, this is Customer Data governed by this DPA; where it belongs to a User's personal Google account, it is personal-tier User Data. Google's Limited Use requirements apply to this data in either case, as described in the Google Workspace Integrations section of the Privacy Policy;
- CRM objects. Where Customer connects Salesforce, Heyou reads account, opportunity, opportunity-contact-role, contact, lead, user, activity (task and event), and contract records to improve recommendation relevance and measure outcomes. Heyou stores a narrowed projection of these records rather than a copy: identifiers, ownership, lifecycle and stage values, and timestamps. Email addresses are not stored in readable form, and activity records are reduced to who, what type, and when — Heyou's schema has no field for an activity subject or body;
- Publicly available professional content the User can already see;
- Derived relationship signals;
- Where a User uses a Heyou query channel (Slack, WhatsApp, or Claude): the question the User sends Heyou, any request context sent with it, Heyou's answer, and the identifiers needed to authenticate the User and route the reply, such as Slack user and workspace identifiers, the User's WhatsApp phone number, or the Claude connector account identifier. Queries, request context, and answers are retained only as set out in the Data Retention and Deletion Schedule; routing identifiers are retained for the life of the channel connection, as set out in the Data Retention and Deletion Schedule; and
- Agent-generated content.

Heyou does not process body content from personal-tier sources. Corporate email body content is not processed unless explicitly enabled by Customer for a feature designed for that purpose. These commitments concern a User's communications with other people; they do not restrict Heyou from processing a question

a User addresses to Heyou through a Heyou query channel such as Slack, WhatsApp, or Claude, which Heyou processes in order to answer it.

Records Heyou Writes to a Connected CRM

Where Customer enables it, Heyou writes its own relationship recommendations and their status into records Heyou installs in Customer's CRM under a dedicated namespace. Heyou writes no data to Customer's standard CRM objects. The records carry Heyou-generated content — the recommendation, its reasoning, urgency, status, and any draft message prepared for a User's review — and Heyou's model prompts and internal score components are not written. Customer controls whether this is enabled, and mirrored records in a terminal status are purged on a retention window Customer configures.

7. Presentation of Contact Details

When Heyou presents an email address or phone number to a User, the value is retrieved only from Customer Data, such as organizational systems the Customer connected, or from User Data, such as personal resources the User connected. Heyou does not use third-party enrichment, data-broker sources, or public scraping to obtain or supplement contact details.

8. User-Identified Targets Not in Connected Systems

For individuals identified by a User as a target but not present in Customer connected systems, Heyou processes only the minimum information needed to surface a relationship-path recommendation. Heyou does not contact such individuals on Customer's behalf. Outreach is initiated by the Authorized User through the User's own channels.

9. Special Category Data

Heyou does not intentionally Process special categories of Personal Data under Article 9 GDPR as part of the standard service. Customer must not submit such data unless a feature is expressly designed and contracted for that use.

10. Processor Obligations

Heyou will:

- (a) Process Personal Data only on Customer's documented instructions, including as set out in the Terms of Service, DPA, Order Form, and Customer's use of the Services;
- (b) ensure personnel authorized to Process Personal Data are bound by confidentiality;
- (c) implement appropriate technical and organizational measures;
- (d) assist Customer, at Customer's cost for non-routine requests where permitted by the agreement, with responding to Data Subject requests, Data Protection Impact Assessments, and consultations with supervisory authorities. Where Heyou receives a request directly from an individual about Customer Data, Heyou will promptly forward it to Customer and act on Customer's instructions, and may keep a minimal suppression record to prevent the individual's information from being collected again;

- (e) notify Customer of a Personal Data Breach without undue delay and, where applicable, within 72 hours of becoming aware, providing information reasonably required by Article 33(3) GDPR where available;
- (f) at the end of the Services, provide the Customer Export described in the Terms of Service if Customer requests it, including, at Customer's choice, the return of the organizational-tier Customer Data described there, and then delete Personal Data, including existing copies, unless retention is required by law or the data is part of the recommendation and charge records needed to charge meetings under the Order Form, which hold a recommendation identifier, accounts and dates rather than individuals, for which Heyou is an independent controller as stated in Section 1, and which are kept as set out in the Data Retention and Deletion Schedule. Personal Data that Heyou read from Customer's connected systems remains available to Customer in those systems; and
- (g) make available information necessary to demonstrate compliance and allow for audits as described in this DPA.

11. Subprocessors

Customer grants Heyou general authorization to engage subprocessors. Heyou will: (i) maintain a current subprocessor list; (ii) impose data protection obligations on subprocessors no less protective in substance than this DPA; (iii) remain responsible for subprocessor acts and omissions as required by applicable law and contract; and (iv) update the Subprocessor List and notify Customer by email at least thirty (30) days before a new or replacement subprocessor begins processing Customer Data. Customer may object on reasonable data-protection grounds within the notice period. If the parties cannot agree on a resolution, Customer may terminate the affected Services for cause and receive any applicable refund of prepaid, unused fees.

User-authorized third-party platforms are not subprocessors. Where an Authorized User authorizes Heyou to access a third-party platform using the User's own account or authorization flow, that platform operates the User's account independently and is not engaged by Heyou to process Customer Data on Heyou's behalf. The User's relationship with such platforms is governed directly by the platform's own terms.

The same applies where Customer, rather than an individual Authorized User, authorizes a platform connection at the organizational level, such as installing the Heyou Slack app in Customer's workspace. That platform operates under Customer's own agreement with it and is not engaged by Heyou to process Customer Data on Heyou's behalf. Where instead Heyou operates the channel itself — as with the Heyou-operated WhatsApp business number — the platform is a Heyou subprocessor and appears on the Subprocessor List.

12. International Transfers

Transfers to Heyou in Israel

Transfers from the EEA, UK, or Switzerland to Heyou entities or personnel in Israel may rely on adequacy decisions recognizing Israel as providing an adequate level of data protection, where applicable.

Transfers to Non-Adequate Countries

Where transfers are subject to EU or UK data protection law and the recipient is in a country without an adequacy decision, the parties enter into the applicable Standard Contractual Clauses and UK transfer mechanism as required.

For EU transfers, the parties incorporate Module Two of the EU Standard Contractual Clauses for Controller-to-Processor transfers where applicable. For UK transfers, the applicable UK International Data Transfer Addendum or International Data Transfer Agreement applies where required. For Swiss transfers, the SCCs apply with references adapted to Swiss data-protection law and the FDPIC.

13. Audits

Heyou demonstrates compliance primarily through security and compliance artifacts, which may include:

- ISO/IEC 27001:2022 certificate;
- SOC 2 Type II report when available;
- Penetration test executive summaries;
- Completed security questionnaires; and
- Security Overview and supporting policies.

These materials may be made available under NDA through a trust center or security review process. Where those artifacts are insufficient to address a specific supervisory-authority or regulated-industry requirement, Customer may conduct an audit or mandate a third-party auditor bound by confidentiality no more than once per year, on reasonable notice, during business hours, without disrupting Heyou's operations or other customers, and at Customer's expense unless the audit reveals material non-compliance.

14. Liability

Liability under this DPA is governed by the limitation of liability clause of the Terms of Service, including the Heyou Data Protection Liability cap, except where applicable law does not allow such a limitation.

15. Order of Precedence

In case of conflict, the SCCs prevail over the rest of this DPA with respect to transfers they govern. The DPA prevails over the Order Form, the Terms of Service, and all other documents with respect to Processing of Personal Data; an Order Form may narrow but not widen the purposes, sources, or retention stated here.

Annex II — Technical and Organizational Measures Summary

Tenant Ownership and Isolation

Within Heyou's own database and application layer, Customer Data is processed and stored in a logically isolated tenant. Heyou does not combine Customer Data across tenants in its own systems, does not operate a cross-tenant queryable directory, and does not use Customer Data to build a Heyou-owned contact database or data product. Subprocessors operate their own infrastructure; Heyou imposes contractual data-protection obligations on them but does not control how each subprocessor internally organizes data within its own systems.

User-Tier Isolation

User Data connected from personal resources by an individual Authorized User is held at the User level and is architecturally not available to the Customer, including Customer admins, or to other Authorized Users, except where the User has affirmatively shared specific data with the organization.

Pseudonymization and Encryption

Customer data stores are encrypted at rest using Google-managed encryption or equivalent managed cloud encryption. Network traffic is encrypted in transit using TLS. Secrets are managed through Secret Manager.

PII Minimization Before Third-Party Generative AI Calls

Where identifiers are not required for the task, personal identifiers such as names, emails, and phone numbers may be masked with placeholders before Customer Data is sent to third-party generative AI providers. Outputs are re-associated with original values inside Heyou.

Availability and Resilience

Heyou uses managed cloud infrastructure, backups, monitoring, and operational processes designed to support confidentiality, integrity, availability, and resilience.

Regular Testing

Heyou performs vulnerability scanning, code review, security testing, and third-party penetration testing as part of its security program.

Access Control

Heyou supports SSO, role-based access controls, MFA for internal administrators, least-privilege internal access, and time-bound production access processes.

Incident Management

Heyou maintains documented incident-response runbooks and a customer-notification process for confirmed security incidents involving Customer Data.

Personnel

Personnel are subject to confidentiality obligations, security and privacy training, and access-control processes.

Data Minimization

Heyou follows a metadata-first approach where appropriate. Content access is limited to cases where a feature requires it and the customer has enabled it. Personal-tier message content is not ingested.

Business Continuity

Heyou maintains encrypted backups and disaster-recovery procedures appropriate for the service.