

Acceptable Use Policy

What you commit to when you use Heyou — no spam, no scraping, no high-stakes automated decisioning, and an obligation to honor opt-outs and meet local employee-monitoring requirements.

Version 1.1

Effective 10 May 2026

Last updated 23 October 2026

heyou.io/acceptable-use/

Customer and its Authorized Users must not use Heyou to:

- Violate applicable law, including anti-spam laws, telemarketing laws, anti-bribery laws, sanctions, export controls, privacy laws, or employment laws;
- Send unlawful spam, phishing, harassing messages, or content that is defamatory, hateful, obscene, or otherwise unlawful;
- Access third-party platforms through Heyou in violation of those platforms' terms of service or applicable law, including the Slack API Terms of Service, the Anthropic Software Directory Policy, and the Salesforce AppExchange Program Policies where the corresponding Heyou app, package, or connector is installed;
- Upload malware or attempt to probe, penetrate, disrupt, or degrade the Services or other customers' tenants;
- Reverse engineer, decompile, or disassemble the Services, or attempt to derive source code, algorithms, or non-public interfaces, except as expressly permitted by applicable law;
- Conduct intrusive security testing, penetration testing, or red-teaming without Heyou's prior written consent, except for good-faith vulnerability reporting under Heyou's coordinated disclosure process;
- Use the Services to build, train, or benchmark a competing product or machine-learning model, or copy the Services' user interface;
- Use automated systems, bots, or scrapers to access the Services other than Heyou-provided APIs used in accordance with the Documentation;
- Make decisions that produce legal or similarly significant effects on individuals using outputs of Heyou's AI agents, including hiring, firing, promotion, performance evaluation, compensation, credit, insurance underwriting, immigration, or housing decisions;
- Process special categories of data under Article 9 GDPR or regulated categories such as protected health information, payment card data, or children's data unless a specific Heyou feature is expressly designed and contracted for that use;
- Impersonate any person or entity;
- Exceed documented rate limits or attempt to circumvent technical controls;
- Use the Services to target individuals in ways that would not be lawful for Customer to do directly;
- Connect to Heyou any resource the User does not personally control or is not entitled to connect, such as another person's personal email, messaging account, or device;

- Attempt to access another Authorized User's personal-tier User Data content or signals except to the extent the other User has affirmatively shared specific data with the organization.

Employee Monitoring and Works-Council Regimes

Heyou may process employee email metadata, calendar metadata, directory information, and professional relationship context to map relationship paths. In several jurisdictions this may implicate national employee-monitoring, labor, or works-council requirements in addition to GDPR.

Customer is responsible for putting necessary safeguards in place before enabling Heyou for employees in jurisdictions that require them. These safeguards may include DPIAs, Legitimate Interest Assessments, employee notices, works-council consultation, trade-union agreements, or labor-authority authorization.

Customers operating in jurisdictions with employee-monitoring or works-council regimes should complete applicable consultations or approvals before enabling Heyou for affected employees.

Heyou may provide templates and guidance to assist Customers with these obligations on request. Heyou does not provide legal advice; Customers remain responsible for compliance with their own employment, data-protection, and labor laws.

Honoring Opt-Outs

Customer must promptly honor any data-subject opt-out, deletion request, or objection to processing communicated through Heyou's privacy process, including by removing affected data from Customer's tenant and not re-introducing it through subsequent integration syncs where required.

Violations may result in suspension, termination, and indemnification obligations under the applicable agreement.

Report suspected abuse to dpo@heyou.io.