Pheus.ai — Privacy Policy

Last updated: October 19, 2025

1) Who we are

This Privacy Policy explains how **Pheus.ai** (“Pheus”, “we”, “us”, “our”) collects and processes personal data when you use our website, app, and integrations.

Controller: Sole Entrepreneur Rafayel Baghyan, Saryan 33,9, Yerevan, Armenia, 0002.
Contact: baghyan13@gmail.com

2) What we do

Pheus helps founders and sales teams plan thoughtful outreach and maintain relationships by analyzing signals from the tools you connect (e.g., LinkedIn, email, calendar) and your own notes/knowledge base. We provide suggestions and drafts; you control what gets sent.

3) Data we collect

a) Account & product data you provide

- Profile & contact info (name, email, company, role)
- Workspace settings, goals, ICP definitions, tags, custom notes
- Content you upload (notes, knowledge sources, message templates)

b) Connected-account data (only with your authorization)

- **LinkedIn:** After you sign in with OAuth, we may access permitted fields for the approved product/permission(s) (e.g., OpenID profile/email; posting on your behalf if you enable it). We **never** scrape LinkedIn or store credentials; we store encrypted access tokens.

- **Email/Calendar/CRM/Messaging** (if you connect): header metadata, subjects, participants, scheduled events, and message snippets you explicitly allow; we do not read or store entire mailboxes by default.

- **Events/news/holidays**: industry/country triggers relevant to your contacts.

- **Usage & device data:** logs, IP, browser/OS, crash reports, cookie identifiers.

c) Special categories

We do **not** intentionally collect sensitive data (e.g., health, religion). Please avoid submitting it. If you do, you are responsible for having a lawful basis to share it with us.

4) How we use data (purposes & legal bases)

- **Provide and improve the service** (perform the contract): authenticate you, generate outreach suggestions, maintain features, troubleshoot.
- **Security & abuse prevention** (legitimate interest): detect spam or misuse, protect accounts, audit access.
- **Analytics & product research** (legitimate interest/consent where required): understand feature usage to improve outcomes.
- **Communications** (legitimate interest/consent): service messages, product updates, and marketing (opt-out anytime).
- **Compliance** (legal obligation): honor data subject rights, maintain records.

5) LinkedIn-specific handling

- We access LinkedIn data **only** via officially approved permissions and partner programs (e.g., Open Permissions; Marketing APIs; SNAP, if granted). Most permissions require LinkedIn approval and OAuth 2.0 authentication. Microsoft Learn
- We do **not** scrape LinkedIn or circumvent technical measures.
- **Retention/caching:** We follow LinkedIn's documented limits. For example, member **social activity data** may be stored up to **48 hours**, most **member profile data** from other members up to **24 hours** (cache only), and organization admin/reporting data may be retained longer as specified by LinkedIn's data-storage table. Where multiple limits apply, we use the shortest period. Microsoft Learn
- **Restricted uses:** We will not use LinkedIn **member data** for disallowed use cases (e.g., to create leads or audience lists, ad targeting, recruiting) and will not export or combine member data with third-party datasets in prohibited ways. Microsoft Learn

- If you revoke LinkedIn access or delete your account, we promptly delete LinkedIn-sourced data we hold, subject to legal retention obligations and LinkedIn's terms. Microsoft Learn

6) AI features

Our AI suggests next-best actions and drafts using your authorized data and our knowledge base. We do **not** use your private content to train public models. For any third-party model providers we use as processors, we contractually restrict use to your instructions.

7) Sharing your data

We do **not sell** personal data. We share data with:

- **Processors/sub-processors**: hosting, storage, analytics, email delivery, error monitoring, security (bound by DPAs and confidentiality).
- **Integrations** you connect (e.g., posting via LinkedIn if you instruct us).
- **Legal/Compliance**: if required by law or to protect rights and safety.
  We'll publish and maintain a current list of sub-processors at: **pheus.ai/subprocessors**.

8) International transfers

We use global infrastructure. Where data leaves the EEA/UK, we rely on adequacy decisions or Standard Contractual Clauses and implement supplementary measures.

9) Retention

- **Account data**: for your subscription + up to 24 months after closure (or sooner upon deletion request), unless law requires longer.
- **Content you upload**: until you delete it or close your account.
- **Connected-account data**: as short as necessary to provide features, never beyond LinkedIn's limits for LinkedIn-sourced data (see §5). Microsoft Learn
- **Logs**: typically 12 months (security/debug).

10) Your rights

Depending on your location, you may have rights to access, correct, delete, restrict/opt-out, portability, and to object.
EEA/UK: you may lodge a complaint with your local authority.
California: we honor CPRA rights (access, delete, correct, limit use of sensitive information, opt-out of “sale/sharing”). To exercise rights: privacy@pheus.ai.

11) Security

We apply industry-standard security: encryption in transit/at rest, token vaulting, least privilege, continuous monitoring, and regular access reviews.

12) Children

Pheus is not for individuals under **16**. LinkedIn

13) Changes

We’ll post updates here and adjust the “Last updated” date. Material changes will be notified via email or in-app.

14) Contact

baghyan13@gmail.com • Pheus.ai,
Saryan 33, 9, Yerevan, Armenia, 0002
For LinkedIn data deletion requests: “Contact Us” section below (subject: “LinkedIn Data Deletion”).