Kinlet™ — Privacy Policy

Version 2026-09-25

Last updated: 25 September 2026

Who we are: PurrGiants (sole proprietor, *toiminimi*), Finnish Business ID (Y-tunnus) 2702464-3, Rannanpohja 7A, 91800 Tyrnävä, Finland · contact details in § 10

---

1. The short version

Kinlet helps community operators notice when a member is drifting away, and invites that member back.

To do that, Kinlet reads **activity timestamps and subscription status** from the community platform. **It does not store members' names, usernames, email addresses, profile details, or anything members write in messages or posts.** The only message text it stores is the text of the messages Kinlet itself sends, so the operator can see exactly what was sent.

We have **three different roles**, and this policy keeps them apart:

whose data	who decides	our role
members of a community that uses Kinlet	the community operator	**processor** — we act only on the operator's instructions (§ 2)
customers — the business that installs or buys Kinlet	us	**controller** (§ 3)
payment and accounting records about customers	us, as required by Finnish law	**controller** (§ 3)

If you are a member and want to know what is held about you, or want it removed, contact the operator of your community. They decide; we act on their instruction.

---

2. Community members — we process on the operator's behalf

2.1 What Kinlet reads, and what it keeps

This list is taken from the code.

what	why	stored by Kinlet?
platform member ID (e.g. `mem_...`)	to tell one member from another	**yes** — in the action log, see 2.3
the member's display name or username	shown to the operator next to the member in the app, so they know who it is	no — read fresh each time the app is

what	why	stored by Kinlet?
		opened, never saved
date the member joined	new member or long-standing	no — read fresh on each run
who posted in the community's chat channels, and when (the author's member ID and the time of each member's latest post)	the drift signal: a member who has gone quiet	no — read fresh on each run
whether the membership is cancelling or cancelled	never contact someone who is leaving on purpose	no
trial end date	tell a trial ending from a member going quiet	no
date of a failed payment, if any	a failed card is a fixable problem	no
whether the member has ever paid, their plan's recurring price and currency, and when their paid period ends	the operator's own bill is based on paying members; the "revenue at risk" figure and leaving alerts shown to the operator	no

Kinlet does not store: names, usernames, email addresses, phone numbers, avatars, IP addresses, the content of messages or posts, course answers, or any special-category data. A member's name is only **shown to the operator** in the app, read fresh each time, and is never put into a message or an alert.

⚠ **What passes through without being kept.** The platform's interface returns some fields together with the ones Kinlet needs — for example a member's avatar. When Kinlet reads who posted in a chat channel and when, the platform returns the messages with their text. Kinlet **discards the text immediately; it does not store, analyse or display it.** Email addresses and phone numbers are never returned, because Kinlet does not ask the platform for permission to read them.

2.2 What Kinlet sends to members

When automatic mode is on (the default) or the operator sends a message manually, Kinlet sends a short invitation to the member **through the community platform's own notification system**, addressed to specific members only. Kinlet does not have members' email addresses and does not email them.

⭐ **A standing rule of this product:** a message to a member never mentions, hints at, or implies that their absence was noticed, or that any tracking exists. Software blocks any message that breaks this rule.

On the Large plan, unless the operator switches it off, about **5 %** of discretionary cases are deliberately left alone to measure whether the invitations help. Failed payments are never held back, and nothing is held back on Free or Growth.

2.3 What is stored about members, and for how long

record	contents	kept
action log	member ID · what was done (e.g. "sent a chat invitation") · date · whether it was automatic or the operator · the	**member ID removed after 12 months**, or within **30 days**

record	contents	kept
	message sent · outcome (whether the member did what the message asked within 2 days, and whether they stayed 30 days later)	after the operator uninstalls Kinlet or the service ends — whichever comes first
the same log **after the member ID is removed**	no identifier — it can no longer be linked to anyone	kept for the operator's monthly limit and statistics
leaving-alert log	member ID · whether the alert was about a cancellation or a failed payment · the date — so that the operator is told about the same event only once. The alert itself goes only to the operator and shows the event, the member's monthly price and the days left in their paid period, **not the member's name**	**member ID removed after 12 months**, or within **30 days** after the operator uninstalls Kinlet or the service ends — whichever comes first
measurement log (Large only, when measurement is on)	member ID · that the case was deliberately left alone to measure whether invitations help · the date · whether the member stayed 30 days later	**member ID removed after 12 months**, or within **30 days** after the operator uninstalls Kinlet or the service ends — whichever comes first

Nothing else about members is stored.

2.4 Members' rights

Members' requests (access, erasure, objection and others) go to the community operator, who is the controller. On the operator's request — or on a verifiable request from the member or from Whop — we remove the member's identifier from every record within **30 days**, and tell the operator.

---

3. Customers — data we control

what	source	why	legal basis (GDPR Art. 6)
your platform company ID and the user ID of the person who accepted our terms, the time, and the version of the terms	the app	proof of what was agreed and when	contract (b); legitimate interest in being able to prove it (f)
your **business ID or VAT number**, if given (optional), and your confirmation that you use Kinlet as a business, not as a consumer	you, in the app	showing that Kinlet is sold only to businesses	contract (b); legitimate interests (f) — being able to show who agreed to what
your app settings (automatic/manual, measurement on/off, leaving alerts on/off, price and trial notices already given) and the date your free trial started (from your first acceptance)	you, in the app	to run the service as you chose	contract (b)
payment events from Whop, **reduced before storage** to what bookkeeping needs: payment ID and status, amount, currency, dates, product / plan / membership IDs, the buyer's platform ID and billing country (needed for bookkeeping; Whop handles any	Whop	billing and **statutory bookkeeping**	legal obligation (c) — Finnish Accounting Act

what	source	why	legal basis (GDPR Art. 6)
VAT). Everything else Whop sends — name, username, email address, phone number, billing and shipping address, card details, card fingerprint, verification results and risk score — is dropped and never stored			
membership events from Whop (activated, deactivated), **reduced before storage** to platform IDs, event type, status and dates — name, username, email address, profile picture, checkout answers and the cancellation reason are dropped and never stored	Whop	knowing who has an active subscription	contract (b)
your emails to us	you	support	contract (b); legitimate interest (f)
technical records of requests to our webhook address that failed verification	anyone who sends them	security and fraud prevention	legitimate interest (f)

We never see your full card number. Payment is handled by Whop; we receive Whop's record of the payment, as listed above.

Our hosting provider keeps short-lived technical logs of requests to our servers, which may include IP addresses; we do not add personal data to them.

---

4. Who else processes data

recipient	role	what	where
Supabase (Supabase Pte. Ltd.)	our processor (hosting: database and webhook receiver)	everything we store (§ 2.3, § 3)	**EU — Frankfurt (`eu-central-1`)**
Whop, Inc. — app interface	hosts Kinlet's interface inside Whop; requests reach our API through Whop's proxy	the signed-in user's identity	USA
Whop, Inc.	the community platform and payment provider; an **independent controller** under its own privacy policy, not our processor	members' data originates there; notifications are delivered there; payments are taken there	USA
Google (Gmail)	our email provider	your emails to us	may be processed in the USA; Google LLC is certified under the EU–US Data Privacy Framework
Microsoft (OneDrive)	storage of our accounting records, and an off-site backup of acceptance records and app settings	payment records; customers' acceptance records (company and user ID, time, version,	may be processed in the USA; Microsoft Corporation is certified under the EU–US Data Privacy Framework

recipient	role	what	where
		business confirmation) and app settings	
our accountant, if one is engaged	statutory bookkeeping	payment records	Finland
Anthropic, PBC	helps explain internal monitoring alerts	server diagnostics only — **no member or customer personal data**	USA

We do not sell data. We do not share it with advertisers. We do not use members' data to train machine-learning models.

⭐ **Member data is stored in the EU.** Supabase is a US company, but the database and the webhook receiver run in **Frankfurt**, where the data is stored and primarily processed. Supabase's own subprocessors (listed at supabase.com/legal/customer-resources/subprocessor-list) may process it elsewhere under Standard Contractual Clauses or other safeguards (DPA § 5–6).

---

5. Transfers outside the EU/EEA

Where personal data is transferred outside the EU/EEA, we rely on the European Commission's **Standard Contractual Clauses** or another valid mechanism under Chapter V GDPR. Details per provider: DPA § 5.

---

6. How long data is kept

data	kept
member IDs in the action log and the leaving-alert log	12 months, or 30 days after uninstall / end of service — whichever first
action log without member IDs	while needed for limits and statistics; contains no personal data
acceptance records, business ID, business-use confirmation	6 years from the end of the calendar year in which the customer relationship ended
app settings	while installed, and 12 months after uninstall, so that a reinstall keeps your choices
accounting vouchers, including the payment events they are based on	**6 years** from the end of the calendar year in which the financial period ended
accounts and financial statements	**10 years** from the end of the financial period
membership events from Whop	reduced to IDs, event type, status and time; kept 6 years like the sales records they support
webhook requests that failed verification	their content is not stored at all; only the arrival time, the three signature headers and the rejection reason are kept, for security monitoring
your emails to us	3 years after the matter was closed

⚠ **Accounting records cannot be deleted on request.** Finnish law requires them to be kept and forbids altering them. A deletion request cannot remove a payment record. This is the one place where the law overrides a request, and we say so plainly.

---

7. Your rights

If you are in the EU/EEA you have the right to access, rectify, erase, restrict, port, and object to the processing of your personal data, and to lodge a complaint with a supervisory authority. In Finland that is the Office of the Data Protection Ombudsman (*Tietosuojavaltuutetun toimisto*), tietosuoja.fi.

Members: direct requests to the operator of your community (§ 2.4). **Customers:** contact us (§ 10). We reply within one month.

---

8. Security

- All traffic is encrypted in transit (HTTPS).
- Payment events are cryptographically signed by Whop; we verify every signature and a 5-minute time window, and reject anything that fails.
- Stored payment events cannot be altered, and are removed only when their retention period in § 6 ends; each carries a checksum, so any change would be detectable. Accounting records are kept in a hash chain for the same reason.
- Database tables are closed to every public access role; only the server-side service key can read or write them.
- Access to production data is limited to the operator of this service.

⚠ No service can promise that a breach is impossible. If a breach affects customers' personal data and is likely to result in a risk to their rights, we notify the supervisory authority within 72 hours and inform the affected customers. If it affects members' data, we notify the community operator as described in the DPA § 9.

---

9. Changes to this policy

We post material changes in the app at least **14 days** before they take effect — **30 days** before adding or replacing a subprocessor (DPA § 5).

---

10. Contact

PurrGiants (toiminimi), Y-tunnus 2702464-3
Rannanpohja 7A, 91800 Tyrnävä, Finland
Email: purrgiants@gmail.com