



Privacy Policy

PREM Confidential API

PREM SA · Version 1.1 · Last Updated: 04/09/2026

Our core commitment: API payload data is never stored by PREM. Depending on the model you select, inference runs either (a) within a hardware-sealed Trusted Execution Environment (TEE), where payload is client-side encrypted and technically inaccessible to PREM and to any provider, or (b) via Zero-Data-Retention providers in the EU/EEA or UK, where prompts are processed transiently over encrypted connections (TLS) and neither PREM nor the provider retains, reads beyond what is necessary to provide the Service, or uses payload data for any purpose, including model training, by contractual commitment. See Section 6. Your account and organization data is stored securely in Germany (EU). This policy explains everything we do and do not hold.

1. Who We Are

PREM SA ("PREM", "we", "us", "our") is a company incorporated under Swiss law at Crocicchio Cortogna 6, 6900 Lugano, Switzerland (CHE-371.240.335). We operate the PREM Confidential API (the "Service"), an AI inference platform built on Trusted Execution Environment (TEE) technology.

EU Representative (GDPR Art. 27): PREM AI S.r.l., Via Giuseppe Verdi 12, 70017, Putignano (BA), Italy — designated as PREM SA's EU representative for the purposes of GDPR Art. 27. EU/EEA-based Developers and data subjects may contact PREM AI S.r.l. on all matters relating to GDPR compliance, in addition to contacting PREM SA directly. PREM AI S.r.l. does not independently process Developer or payload data as part of the Confidential API service.

Data protection: privacy@premai.io Security: security@premai.io

2. Scope of This Policy

This Privacy Policy covers all personal data we collect when you register, use, or interact with the Confidential API and its dashboard. It distinguishes clearly between two very different categories of data:

(i) Account and Organization Data: information you provide when signing up, and operational data generated by your use of the Service. This data is stored in our database in Germany (EU). This policy describes it in full.

(ii) API Payload Data: the content of your API requests and responses. This data is processed exclusively within the TEE and is never stored by PREM. It is outside the scope of this policy beyond confirming that we cannot access it.

Where you use the Service to process personal data on behalf of your own users, you are the Data Controller and PREM acts as your Data Processor. That relationship is governed by our **Data Processing Agreement (DPA)**, which you must execute before processing personal data through the API.

Special-category data (GDPR Art. 9 / FADP Art. 5(c)): The Confidential API is not designed for processing health data, biometric data, genetic data, or other special-category personal data. If such data appears in API payloads, PREM processes it transiently under the same architecture, but PREM acting as Processor does not supply the legal basis for that processing. Developers who submit special-category data through the API must: (i) have a valid Art. 9(2) legal basis for that processing; (ii) notify PREM at privacy@premai.io before commencing such use; and (iii) execute a DPA addendum covering special-category processing. Using the API to process special-category data without these measures in place is a breach of the Terms of Service.

3. Applicable Law

This Privacy Policy is designed to comply with:

- (i) Swiss FADP (FADP):** we are established in Switzerland and process personal data of Swiss residents.
- (ii) EU GDPR:** our primary database is in Germany (EU). We process personal data of EU/EEA residents and offer services directed at the EU market.

Where multiple laws apply to the same processing activity, we apply the stricter standard.

4. What Data We Collect and Store

Key fact: payload data is never stored. PREM does not collect, store, or log the content of your API requests or responses. Payload data is processed transiently within the TEE and discarded once the response is returned. The tables below cover only the account and organization data that PREM does store.

4.1 User Account Data

Stored in our database in Germany (EU). Retained for the duration of your account plus 90 days after closure.

Data element	What it is	Can PREM read it in plaintext?
Email address	Your registration and login email	Yes
Name / surname	Your full name as provided at registration	Yes
Password	Your login credential	No — stored as a cryptographic hash using OWASP-compliant methods and SOC 2-certified processes. PREM cannot recover or read your password.

Data element	What it is	Can PREM read it in plaintext?
Organization memberships	The organizations your account belongs to	Yes
Pending invitations	Organization invitations you have received	Yes
Security identifiers	IP address, device/session identifiers used for security checks	Yes

4.2 Organization Data

Data associated with your organization account. Stored in our database in Germany (EU).

Data element	What it is	Can PREM read it in plaintext?
Organization name	The name of your organization	Yes
Account balance	Current prepaid credit balance	Yes
Stripe invoice IDs	References to Stripe invoices (identifiers only — no card data held by PREM)	Yes
Amounts paid	Payment amounts recorded against your account	Yes
Usage statistics	Aggregated operational metrics: model response times, API call counts, error rates	Yes

4.3 Automatically Collected Technical Data

Data element	Purpose	Can PREM read it?
Request metadata	Timestamps, endpoint called, request/response size in bytes (not content), token count, routing region	Yes — used for billing and rate limiting
Technical logs	IP address, SDK version, error codes	Yes — used for security monitoring and debugging

4.4 Data PREM Never Has Access To

Zero access — by design: The following is never visible to PREM or its employees, regardless of circumstances.

(i) API payload content: your prompts, model inputs, and AI-generated responses. Processed transiently within the TEE. Not written to disk, not retained in logs, not accessible to PREM infrastructure operators. Discarded immediately after the response is returned.

(ii) Your password in plaintext: PREM stores only a cryptographic hash. Your actual password is never transmitted to or stored by PREM's systems in recoverable form.

(iii) Your encryption keys (KEK / DEK): client-side encryption using XChaCha20-Poly1305 is the only method by which the API can be used. You always hold the master key (KEK). PREM has no technical ability to decrypt your payload data under any circumstances. This is an architectural property, not a policy choice.

(iv) Your financial card data: Stripe processes all card transactions. PREM receives only Stripe invoice IDs, payment amounts, and limited card details (specifically the card's country of origin, expiration date, and the last four digits) — never full card numbers, CVV, or full billing addresses.

5. How We Use Your Data

Processing activity	Data used	Legal basis
Provide the Service — account management, authentication, API routing	Account data, security identifiers	Performance of contract
Billing — calculate usage fees and issue invoices	Organization balance, Stripe invoice IDs, amounts paid, usage statistics	Performance of contract
Security — rate limiting, abuse prevention, fraud detection	Security identifiers, request metadata, technical logs	Performance of contract / Legitimate interest
Legal compliance — respond to lawful regulatory requests	Minimum data required by applicable law	Legal obligation
Service improvement — aggregated, anonymized analysis only	Usage statistics — anonymized before any analysis. Payload data never used.	Legitimate interest

We **do not**: use payload data to train AI models; use payload data for analytics, model improvement, or any secondary purpose whatsoever — this prohibition extends to anonymized or aggregated patterns derived from payload sessions; sell your personal data or personal information; share your personal information for cross-context behavioral advertising; serve advertising; or profile users for automated decisions producing legal or significant effects.

6. Sub-Processors and Data Sharing

We work with two categories of sub-processors:

(a) Enclave sub-processors — payload is client-side encrypted and decrypted only within a hardware-sealed Trusted Execution Environment (TEE). Neither PREM nor the provider can technically access payload content in plaintext.

(b) Zero-Data-Retention (ZDR) inference providers — prompts and completions are transmitted over encrypted connections (TLS) and processed in plaintext transiently, solely to perform inference. Neither PREM nor the ZDR provider retains, logs, stores, or uses payload data for any purpose (including model training); this is a contractual commitment under the applicable DPA. Processing occurs on EU/EEA or UK infrastructure.

6.1 Platform Sub-Processors

Sub-processor	Role	Data shared	Location
Stripe	Payment processing, fraud prevention, and usage-based billing	Billing data and amounts paid only. No payload data.	US / EU
Cloudflare	CDN, DDoS protection, traffic routing	Request metadata only (not content)	Global
Hetzner	Hosting of account and organization data	Account and organization data	Germany (EU)
PREM AI S.r.l.	GDPR Art. 27 EU Representative only — no data processing role in the Confidential API	No data shared for processing purposes. Contact point only.	Italy (EU)

6.2 Enclave Sub-Processors

Sub-processor	Role	Data shared	Location
Soleblanca SA	Hardware hosting for enclave processing	Client-side encrypted payload only; inaccessible to provider in plaintext	Europe / United Kingdom / Switzerland

6.3 Zero-Data-Retention Inference Providers

Sub-processor	Role	Data shared	Location
Nebius B.V.	AI inference provider	AI prompts and completions, processed transiently for inference only; zero retention per DPA ; no training use	EU/UK
TensorX	AI inference provider	AI prompts and completions, processed transiently for inference only; zero retention per DPA ; no training use	Ireland (EU)

Payload data is never sold, used for model training, or shared for any purpose other than providing the Service. Payload content is accessible in plaintext to the ZDR inference providers listed above and strictly during the inference operation. Enclave sub-processors never have plaintext access.

Current sub-processor list available on request at privacy@premai.io.

6A. Government and Law Enforcement Access

We cannot produce what we do not hold: API Payload Data is not stored by PREM. If PREM receives a lawful order requiring production of Payload Data, PREM will inform the requesting authority that such data is not held by PREM in recoverable or accessible form — because it is not. This is a technical and architectural fact, not a legal position.

Where PREM receives any government or law enforcement request relating to Developer Data (account or organization data):

- (i) PREM will assess the legal validity of the request before complying.
- (ii) PREM will notify Developer before producing any Developer Data in response to such a request, unless prohibited from doing so by law or court order.
- (iii) Where notification is prohibited, PREM will: (a) seek to challenge the prohibition; (b) provide Developer with as much information as it legally can; and (c) disclose only the minimum data required to comply.
- (iv) PREM will not voluntarily produce Developer Data to any government authority without a binding legal order.

7. International Data Transfers

Germany (EU) — default exchange point for all requests: every API request is routed through PREM's infrastructure in Germany, regardless of which jurisdiction the AI model runs in. Germany is the consistent entry and exit point for all API traffic. Account and organization data is also stored in Germany. Switzerland has an EU adequacy decision, so transfers from PREM SA to Germany are compliant without additional transfer mechanisms.

AI model routing across jurisdictions: AI model inference may occur on infrastructure in multiple jurisdictions. However, all payload data is client-side encrypted with the Developer's KEK before leaving the

Developer's device, and remains encrypted throughout processing. PREM and any infrastructure provider have zero access to plaintext payload content regardless of the jurisdiction of processing.

Region locking: Developers who require processing to be locked to a specific region (for example, EU-only) may request this from PREM. Region locking is not tier-based. It is available on request at any plan level.

CH→US (PREM LABS INC — infrastructure layer): to the extent any technical infrastructure involves PREM's US entity, transfers from PREM SA to PREM LABS INC are governed by Standard Contractual Clauses (Module 3, Processor-to-Processor). Mandatory client-side encryption (XChaCha20-Poly1305) serves as a supplementary technical measure under the Schrems II framework — payload data is encrypted with keys held exclusively by Developer and is inaccessible to any party including PREM LABS INC.

Payment processing (Stripe): billing data is shared with Stripe in accordance with Stripe's Data Processing Agreement and applicable transfer mechanisms.

8. Data Retention

Data type	Retention period	Notes
API Payload Data	Zero — not retained	Processed transiently in TEE; discarded once response is returned. Nothing to retain or delete.
User account data (email, name, etc.)	Account lifetime + 90 days	You have 30 days after account closure to request export of account data.
Hashed password	Account lifetime + 90 days	Hash only — original password never recoverable.
Organization data (name, balance, invoice IDs)	Account lifetime + 90 days (except amounts paid)	
Billing records and amounts paid	10 years	Required by Swiss OR Art. 958f and applicable tax law.
Usage statistics	12 months, then anonymized and aggregated	Anonymized data may be retained for service improvement. See anonymization note below.
Technical logs	90 days	
Support correspondence	3 years from last communication	

Anonymization: usage statistics retained beyond 12 months are anonymized by removal of all direct and indirect identifiers (account ID, organization ID, IP address, API Key reference), rendering re-identification impossible. Anonymized data does not constitute personal data under FADP or GDPR and is retained indefinitely for service improvement only.

9. Your Rights

9.1 Rights Under FADP and GDPR

Under the Swiss FADP and GDPR, you may:

- (i) Access:** confirm whether PREM holds personal data about you and receive a copy (GDPR Art. 15 / FADP Art. 25).
- (ii) Rectification:** correct inaccurate data (GDPR Art. 16 / FADP Art. 32).
- (iii) Erasure:** request deletion where PREM no longer has a legal basis to retain data (GDPR Art. 17 / FADP Art. 32).
- (iv) Restriction:** restrict processing in certain circumstances (GDPR Art. 18).
- (v) Portability:** receive your data in a structured, machine-readable format (GDPR Art. 20 / FADP Art. 28).
- (vi) Objection:** object to processing based on legitimate interest (GDPR Art. 21 / FADP Art. 32).
- (vii) Withdraw consent:** where processing is consent-based (GDPR Art. 7(3)).

To exercise these rights: privacy@premai.io. We respond within 30 days for FADP/GDPR requests.

To lodge a complaint:

Switzerland — FDPIC: www.edoeb.admin.ch · +41 58 462 43 95

EU/EEA: your local supervisory authority (GDPR Art. 77). For Germany: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), www.bfdi.bund.de

Regarding payload data: Because API payload data is never stored by PREM, requests to access, correct, or delete payload data cannot be fulfilled — there is nothing in our systems to produce or delete. You hold full control over your payload data at source.

9.2 Developers Located in the United States

If you are located in the United States, PREM processes only limited professional data about you as described in Section 4. The rights in Section 9.1 (access, rectification, erasure, portability, objection) apply to you regardless of your location and provide equivalent or greater protections to those available under US state privacy laws. To the extent any applicable US state privacy law applies to PREM's processing of your data, you may exercise your rights through the same channel: privacy@premai.io. PREM does not sell personal data and does not use it for targeted advertising or cross-context behavioral advertising. We will review this section as PREM's scale of US operations develops.

10. Security

PREM implements the following technical and organizational security measures:

- (i) TEE / Confidential Compute:** payload data is processed within hardware-sealed enclaves inaccessible to PREM's infrastructure operators, cloud providers, or any third party.
- (ii) Password hashing:** passwords are stored as cryptographic hashes using OWASP-recommended algorithms (bcrypt / Argon2 or equivalent). PREM cannot recover passwords in plaintext. This is verified under our SOC 2 program.
- (iii) Encryption in transit:** all connections use TLS 1.2 or higher.
- (iv) Encryption at rest:** account and organization data is stored encrypted at rest in our German database.
- (v) Access controls:** MFA and role-based access control (RBAC) on all PREM production systems.
- (vi) SOC 2 Type II:** PREM is working toward SOC 2 Type II certification. Security controls are audited independently. Our security practices are aligned with SOC 2 requirements throughout.
- (vii) Vulnerability management:** regular vulnerability scans and annual penetration testing.
- Security vulnerability disclosures: security@premai.io (subject: "Security Disclosure").

11. Data Breach Notification

If PREM becomes aware of a personal data breach affecting account or organization data:

- (i) Regulatory notification:** we notify the FDPIC (Switzerland) and the BfDI (Germany, as the database location) as soon as possible as required by FADP Art. 24, and within 72 hours as required by GDPR Art. 33.
- (ii) Individual notification:** where the breach poses a high risk to your rights and freedoms, we notify you without undue delay.

Note: because API payload data is never stored by PREM, a security breach of PREM's account infrastructure cannot expose payload content — there is none to breach.

12. Cookies and Tracking

The Service uses only strictly necessary cookies. We do not use analytics cookies, advertising trackers, or third-party tracking scripts.

Cookie / Service	Purpose	Duration
Session / Auth	Authentication and session management	1 year
Cloudflare	Security, bot protection, and traffic management	1 year
Stripe	Fraud prevention during payment processing	1 year

No consent banner is required for strictly necessary cookies. You may disable cookies via browser settings; this will prevent the Service from functioning correctly.

13. Children

The Service is not intended for individuals under 16. We do not knowingly collect personal data from children. Contact privacy@premai.io if you believe a child has provided data to PREM.

14. Changes to This Policy

We may update this Privacy Policy from time to time. Material changes will be communicated via email or in-service notification at least 30 days before taking effect. The "Last Updated" date at the top reflects the most recent revision. Continued use of the Service after a material change takes effect constitutes acceptance.

15. Contact

General support	support@premai.io
Data protection and privacy rights	privacy@premai.io (subject: "Data Protection Request")
Security disclosures	security@premai.io (subject: "Security Disclosure")
Postal address	PREM SA, Contrada di Sassello 5, 6900 Lugano, Switzerland
EU Representative (GDPR Art. 27)	PREM AI S.r.l., Via Giuseppe Verdi 6, 70017, Putignano (BA), Italy · privacy@premai.io
Swiss supervisory authority (FDPIC)	www.edoeb.admin.ch · +41 58 462 43 95
German supervisory authority (BfDI)	www.bfdi.bund.de · +49 228 997799 0
Italian supervisory authority (Garante)	www.garanteprivacy.it · +39 06 696771

This Privacy Policy is provided in English. In case of conflict between translated versions and the English version, the English version prevails.