



Terms of Service

PREM Confidential API

PREM SA · Version 1.1 · Last Updated: 04/09/2026 · Governing law: Swiss (Code of Obligations)

Before you use the API: By creating an account, accessing the dashboard, or using the PREM Confidential API, its SDK, or related tools, you agree to be bound by these Terms. If you are acting on behalf of an organization, you confirm you have authority to bind that organization. If you do not agree, do not use the Service.

Article 1 — Definitions

In these Terms, the following definitions apply:

"Service" / "API" The PREM Confidential API, including all endpoints, SDKs, documentation, dashboard, and related developer tools provided by PREM SA.

"PREM" / "we" / "us" PREM SA, incorporated under Swiss law at Contrada di Sassello 5, 6900 Lugano, Switzerland (CHE-371.240.335).

"Developer" / "you" The individual or legal entity accepting these Terms and using the Service.

"Account" The developer account created to access the Service.

"API Key" The unique credential issued by PREM to authenticate Developer API requests.

"KEK (Key Encryption Key)" The master encryption key generated and held exclusively by Developer for client-side encryption and decryption.

"DEK (Data Encryption Key)" A per-session encryption key derived or wrapped by the KEK.

"TEE" / "Enclave" / "CVM" A Confidential Virtual Machine using hardware-enforced Trusted Execution Environments (e.g., Intel TDX, AMD SEV, NVIDIA Confidential Computing) where Payload Data is processed.

"Attestation"	A cryptographic verification process that proves the integrity and configuration of the enclave environment, allowing Developers to independently verify what code is running in the TEE.
"Payload Data"	The data, prompts, model inputs, AI responses, and any other content submitted by Developer to the API for processing. Payload Data is never stored by PREM.
"Output"	The processed result returned by the API in response to a Payload Data submission.
"Developer Data"	Account data, organization data, usage metadata, billing data, and support communications as described in the Privacy Policy. Does not include Payload Data.
"DPA"	The PREM Confidential API Data Processing Agreement, governing PREM's processing of personal data as Data Processor on Developer's behalf.
"Privacy Policy"	The PREM Confidential API Privacy Policy, available at https://dashboard.prem.io/legal/privacy , which describes how we handle Developer Data, the Germany (EU) database location, data retention practices, and the PREM AI S.r.l. EU representative designation under GDPR Art. 27.
"Processing Path"	The inference route applicable to a given model or endpoint: either (a) the "Enclave Path", where Payload Data is client-side encrypted and processed within a TEE; or (b) the "ZDR Path", where Payload Data is transmitted over TLS and processed transiently by PREM and Zero-Data-Retention inference providers in the EU/EEA or UK (listed in the Privacy Policy), which are contractually prohibited from retaining, logging, or using Payload Data for any purpose, including model training. The applicable Processing Path for each model is identified in the API documentation.
"SLA"	The Service Level Agreement published at docs.prem.ai/legal/sla .
"Personal Data"	Any information relating to an identified or identifiable natural person, as defined under the Swiss FADP and EU GDPR.

Article 2 — Description of the Service

1. PREM provides an AI inference platform featuring: OpenAI-compatible API endpoints for chat completions, audio transcription, and audio translation; and, depending on the model or endpoint selected by Developer, either the Enclave Path (mandatory client-side encryption using XChaCha20-Poly1305; hardware-enforced processing within TEEs; self-hosted, in-house operated AI models) or the ZDR Path (TLS-encrypted transmission to Zero-Data-Retention inference

providers in the EU/EEA or UK, which process Payload Data transiently and are contractually prohibited from retaining, logging, or using it for any purpose, including model training). On the Enclave Path, PREM does not forward Payload Data to third-party AI providers.

2. On the Enclave Path, all AI model processing occurs within hardware-sealed enclaves and PREM cannot access the plaintext content of Developer requests or responses at any point. On the ZDR Path, Payload Data is transiently accessible in plaintext to PREM and the ZDR provider during inference; PREM commits, and requires each ZDR provider to commit by contract (DPA), to no retention, no logging, no training use, and no access beyond what is necessary to provide the Service. In both cases, Payload Data is never stored by PREM after the response is returned.
3. **Cryptographic attestation:** the TEE generates a cryptographic attestation for each session, allowing Developer to independently verify that: (a) the correct code is running in a genuine hardware enclave; (b) the enclave has not been tampered with; and (c) PREM's privacy guarantees are technically enforced rather than merely promised. Attestation endpoints are documented in the API documentation. Attestation applies to the Enclave Path only.
4. **Traffic routing and data location:** every API request is routed through PREM's infrastructure in Germany (EU), which is the default exchange point for all API traffic regardless of where AI model inference occurs. Account and organization data is also stored in Germany. On the Enclave Path, AI model inference may occur on infrastructure in multiple jurisdictions, but payload data is client-side encrypted with Developer's KEK at all times and is inaccessible in plaintext to any party. On the ZDR Path, Payload Data is encrypted in transit (TLS) and processed transiently on EU/EEA or UK infrastructure; it is not client-side encrypted end-to-end. Developers who require processing to be locked to a specific region may request region locking from PREM — this is available at any plan level, not tier-based. See the Privacy Policy for full data residency and transfer details.

Article 3 — Account Registration and Security

3.1 Account Creation

Developer must create an Account to use the Service and must provide accurate, complete registration information, keeping it current throughout the term of these Terms.

3.2 API Keys and Encryption Keys

Upon registration, Developer generates an API Key and, if activating client-side encryption, a KEK. Developer is solely responsible for: (a) safeguarding the API Key, KEK, and any derived keys; (b) all activity occurring under Developer's Account and API Key; (c) maintaining secure backups of all keys. Accounts may not be shared.

Critical — key recovery is impossible: PREM cannot recover Developer's KEK or decrypt Developer's Payload Data if the key is lost. PREM cannot recover passwords — they are stored only as cryptographic hashes. Loss of the KEK results in permanent loss of access to data encrypted with it.

3.3 Account Security

Notify PREM immediately at security@premai.io upon any suspected unauthorized access to the Account or API Key. PREM is not liable for losses from unauthorized use of Developer's credentials.

Article 4 — Trusted Execution Environment and Payload Data

Core warranty: PREM warrants that (a) on the Enclave Path, Payload Data is processed exclusively within a hardware-sealed TEE and PREM personnel and infrastructure cannot access Payload Data in plaintext; and (b) on the ZDR Path, neither PREM nor any ZDR provider retains, logs, stores, or uses Payload Data for any purpose other than processing the specific API request (including no AI model training), and processing occurs solely on EU/EEA or UK infrastructure. This is a legally binding warranty, not a product description. Breach of this warranty is subject to the Super Cap set forth in Article 11.

1. PREM warrants and represents, as of these Terms and throughout Developer's use of the Service:

(a) No plaintext access (Enclave Path): the Service architecture is designed such that PREM personnel and systems cannot access Payload Data in plaintext at any point. PREM's own staff, infrastructure administrators, and cloud providers have no access to Payload Data within the TEE.

(b) No payload storage: Payload Data is processed transiently on the applicable Processing Path. Once the Output is returned to Developer, no copy of the Payload Data remains on PREM's infrastructure or on any sub-processor's infrastructure. Payload Data is not written to disk, retained in logs, or held in any persistent storage.

(c) No secondary use: neither PREM nor any sub-processor uses Payload Data to train AI models, for analytics, for product improvement, or for any purpose other than processing the specific API request that submitted it.

(d) Mandatory client-side encryption: client-side encryption using XChaCha20-Poly1305 is the only method by which the API can be used. Developer always holds the master encryption key (KEK). PREM has no technical ability to decrypt Payload Data under any circumstances. Client-side encryption applies to the Enclave Path only. On the ZDR Path, Payload Data is protected by TLS in transit and by contractual zero-retention obligations.

(e) Cryptographic verifiability: the TEE generates attestation reports allowing Developer to cryptographically verify that the processing environment matches the code published by PREM, without relying solely on PREM's contractual commitments. Attestation applies to the Enclave Path only.

2. Architecture change procedure: any proposed change to the Service architecture that would affect the warranties in clause 4.1(a)–(e) requires written notification to Developer at least 30 days before implementation, with a description of the change and its impact. For enterprise Developers with an executed DPA, prior written consent is required.

3. **Developer responsibility for Payload Data:** Developer is the Data Controller for Payload Data and personal data of Developer's end users submitted through the Service. Developer is responsible for: (a) ensuring a valid legal basis for processing personal data through the Service; (b) providing appropriate privacy notices to Developer's end users; (c) compliance with applicable data protection law.

Article 5 — Data Processing Agreement

1. Where Developer uses the Service to process personal data on behalf of Developer's users or customers, Developer must execute the PREM Confidential API Data Processing Agreement (DPA) before commencing such processing.
2. The DPA governs PREM's processing of personal data as Data Processor. It records: the Germany (EU) location of Developer Data; the TEE processing mechanism for Payload Data; the Standard Contractual Clauses (Module 3) covering any CH→US infrastructure data flows; and PREM's technical and organizational measures (TOMs). In the event of conflict between these Terms and the DPA with respect to the processing of personal data, the DPA prevails. The DPA also records the ZDR Path processing mechanism, the identity of the ZDR inference sub-processors, and their zero-retention, no-training, and EU/EEA/UK-only processing obligations.
3. Developer represents and warrants that it will comply with all applicable data protection law in its use of the Service, including obtaining all required consents or relying on other valid legal bases for processing personal data through the Service.

Article 6 — Acceptable Use

6.1 Permitted Use

Developer may use the Service to build, test, and operate applications and services for Developer's own business purposes or for Developer's customers, provided such use complies with these Terms and applicable law.

6.2 Prohibited Conduct

Violations may result in immediate account suspension or termination without prior notice.

- (i) Use the Service for any unlawful, harmful, or fraudulent purpose.
- (ii) Submit content that is illegal, infringes third-party intellectual property rights, facilitates illegal activity, or constitutes child sexual abuse material (CSAM), terrorism-related content, or content intended to harm individuals.
- (iii) Attempt to circumvent, probe, or attack the TEE, encryption systems, authentication, or rate limits.

- (iv) Reverse-engineer, decompile, or disassemble the Service, SDK, or enclave software, except as permitted by applicable law.
- (v) Use the Service to develop competing products substantially based on PREM's TEE architecture or enclave design.
- (vi) Share, resell, or sublicense API access to third parties without PREM's prior written consent.
- (vii) Interfere with or disproportionately burden the Service or its infrastructure.
- (viii) Cryptocurrency mining or similar workloads: use the Service — including its GPU infrastructure — for cryptocurrency mining, proof-of-work computations, or any workload whose primary purpose is to earn external tokens, credits, or financial incentives from third-party networks, without PREM's prior written authorization.
- (ix) Use the Service for mass surveillance, non-consensual individual tracking, or building social credit scoring systems.
- (x) Generate deceptive political content, disinformation, or non-consensual intimate imagery.

6.3 Special-Category and Sensitive Data

The Confidential API is not designed for processing health data, biometric data, genetic data, or other special-category personal data within the meaning of GDPR Art. 9 and FADP Art. 5(c). Where Developer submits special-category data through the API:

- (i) Legal basis:** Developer must have a valid legal basis under GDPR Art. 9(2) / FADP Art. 31 for that processing before submitting such data. PREM acting as Data Processor does not supply this legal basis.
- (ii) Prior notification:** Developer must notify PREM at privacy@premai.io before commencing any use of the API that involves special-category personal data.
- (iii) DPA addendum:** Developer must execute a DPA addendum covering special-category data processing before commencing such use. PREM reserves the right to decline to enter into such an addendum.
- (iv) Non-compliance:** using the API to process special-category data without the above measures in place is a material breach of these Terms and may result in immediate account suspension.
- (v) HIPAA:** US-based Developers subject to HIPAA who use the API to process protected health information (PHI) must execute a Business Associate Agreement (BAA) with PREM in addition to the DPA addendum. Contact privacy@premai.io to initiate the BAA process.

6.4 EU AI Act Compliance

Developer is the AI *deployer* or *provider* (as applicable) under the EU AI Act for applications built on the Service. PREM's provision of the Service as infrastructure does not transfer these obligations to PREM. Developer must not deploy a high-risk AI system (Annex III) using the Service without implementing the required compliance measures: human oversight mechanisms, accuracy and robustness documentation, and conformity assessment where applicable.

6.5 Export Controls and Sanctions

Developer must comply with all applicable export control laws, including the US EAR. Developer represents and warrants that:

- (i) Developer is not located in, or a national or resident of, any country subject to comprehensive US sanctions (Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine).
- (ii) Developer is not listed on the OFAC SDN List, the BIS Entity List, or the BIS Denied Persons List.
- (iii) Developer will not use the Service in violation of any applicable export control or sanctions laws.
- (iv) Developer must also comply with applicable EU restrictive measures (Council Regulations under CFSP) and Swiss sanctions under the Embargogesetz (EmbG) as administered by SECO. Developer represents that it is not listed on any applicable EU or Swiss sanctions list.

Article 7 — Pricing, Billing and Payment

7.1 Usage-Based Prepaid Model

The Service operates on a prepaid, usage-based billing model. Developer must maintain a positive account balance to use the Service. Current pricing is published on the dashboard and at docs.prem.io/developer-resources/billing/models-and-pricing. Usage fees are deducted from the account balance as API requests are made.

7.2 Payment

Payments are processed through Stripe. By making a payment, Developer also agrees to Stripe's Terms of Service (stripe.com/legal). Account balances are credited immediately upon successful payment. Auto top-up may be enabled at Developer's discretion to maintain a positive balance automatically.

7.3 Usage Tiers and Rate Limits

Access tiers are determined by cumulative spending and account age, providing different rate limits for requests, tokens, concurrent connections, and audio processing:

Tier	Qualification	Rate limit level
Base	New accounts	Standard
Tier 1	Qualifying spend threshold 1	Enhanced
Tier 2	Qualifying spend threshold 2	High
Tier 3	Qualifying spend threshold 3	Premium

Current tier thresholds and rate limit details are published on the dashboard. PREM reserves the right to modify tier thresholds on 30 days' prior notice.

7.4 Fee Updates

PREM may update fees on 60 days' prior written notice. Continued use after the effective date constitutes acceptance. If Developer does not accept updated fees, Developer may close the Account before the effective date and any remaining balance will be handled per clause 7.5.

7.5 Refunds

Prepaid balances are generally non-refundable. Exceptions may be granted at PREM's discretion on a case-by-case basis (Refund requests: support@premai.io). However, if Developer exercises its right to close the Account prior to the effective date of a fee update pursuant to clause 7.4, PREM will refund any unused prepaid balance to Developer pro-rata. If PREM terminates the Service generally with 90 days' notice (see Article 12), unused prepaid balances will also be refunded pro-rata.

7.6 Taxes

All prices are exclusive of applicable VAT and other taxes. Developer is responsible for any taxes, duties, or levies in Developer's jurisdiction.

Article 8 — Intellectual Property

1. PREM retains all intellectual property rights in the Service, including the platform, APIs, SDK, documentation, enclave software, TEE architecture, and all associated improvements. Nothing in these Terms transfers any intellectual property rights to Developer.
2. Developer retains all intellectual property rights in Payload Data and Outputs. By using the Service, Developer grants PREM a limited, non-exclusive, royalty-free license to process Payload Data solely for the purpose of providing the Service. This processing occurs on the applicable Processing Path as described in Article 4.
3. Output generated by AI models in response to Developer's Payload Data is owned by Developer, subject to applicable law and any third-party IP rights in the relevant jurisdiction. **PREM makes no warranty that AI-generated Outputs are free of third-party IP claims.** Developer is solely responsible for evaluating the legal status of Outputs before commercial use.
4. Any feedback or suggestions Developer provides about the Service may be used by PREM without obligation or compensation to Developer.
5. **Platform IP Indemnification:** PREM will defend, indemnify, and hold harmless Developer against any third-party claim alleging that the Service platform, TEE architecture, or enclave software provided by PREM (expressly excluding Developer's Payload Data or any AI-generated Outputs) infringes a valid third-party intellectual property right. Developer must notify PREM promptly of any such claim and grant PREM sole control over the defense and settlement thereof.

Article 9 — Service Levels and Maintenance

1. PREM targets the availability levels set out in the SLA. The SLA is incorporated into these Terms by reference.
2. Scheduled maintenance will be announced at least 48 hours in advance on the API status page at status.prem.io. Emergency maintenance may be performed without prior notice where necessary to protect infrastructure security or data integrity.
3. Available AI models may change over time. PREM will provide at least 30 days' notice before removing a model that is currently generally available.

Article 10 — Warranties and Disclaimers

1. **PREM warrants:** (a) it has the right to provide the Service; (b) the Processing Paths will function as described in Article 4; (c) PREM maintains appropriate security measures as described in the Privacy Policy and the DPA TOMs.
2. **Developer warrants:** (a) it has authority to enter into these Terms; (b) its use of the Service complies with applicable law; (c) Payload Data does not violate any third party's rights; (d) Developer has a valid legal basis for any personal data in Payload Data.
3. Save as expressly stated, the Service is provided on an "as is" basis. PREM does not warrant that the Service will be error-free, uninterrupted, or that Outputs will be accurate, complete, or fit for any particular purpose.
4. **AI output disclaimer:** AI-generated Outputs are provided for informational purposes only and may be inaccurate, incomplete, or biased. Developer is solely responsible for independently evaluating and verifying Outputs. The Service is not a substitute for professional advice and must not be used as the sole basis for decisions with legal, medical, financial, or safety implications. All Outputs must be reviewed by a qualified professional before being relied upon.

Article 11 — Liability

1. Nothing in these Terms limits or excludes either party's liability for: (a) death or personal injury caused by negligence; (b) fraud or fraudulent misrepresentation; (c) any other liability that cannot be limited under Swiss law.
2. **TEE Warranty and Data Storage Breach — Super Cap:** Notwithstanding the general liability cap below, PREM's aggregate liability for direct losses arising out of or relating to a breach of the warranties set forth in Article 10.1(b) (TEE functioning), Article 4.1(b) (no payload storage), or Article 4.1(c) (no secondary use) shall not exceed two (2) times the total fees paid by Developer to PREM in the 12 months immediately preceding the event giving rise to the claim. Under no circumstances shall PREM's liability for such breaches be uncapped.

3. Subject to clauses 11.1 and 11.2, PREM's aggregate liability to Developer under or in connection with these Terms shall not exceed the total fees paid by Developer to PREM in the 12 months immediately preceding the event giving rise to the claim.
4. Neither party shall be liable for indirect, special, incidental, or consequential losses, including loss of profits, revenue, data, or business opportunity, whether or not foreseeable or whether or not the party has been advised of the possibility of such damages.
5. Developer shall indemnify PREM against claims, losses, and expenses (including reasonable legal fees) arising from: (a) Developer's breach of these Terms; (b) Developer's violation of applicable law or third-party rights; (c) the content of Payload Data; or (d) Developer's AI applications built on the Service.

Article 12 — Term and Termination

1. These Terms commence when Developer first creates an Account and continue until terminated.
2. Developer may close the Account at any time by contacting support@premai.io or through the dashboard. Upon closure, API access ceases and any remaining balance is handled per clause 7.5.
3. PREM may suspend or terminate Developer's Account: (a) immediately, for material breach of these Terms, prohibited use, illegal activity, or sustained failure to maintain a positive balance; (b) with 30 days' written notice, for any other reason.
4. PREM may discontinue the Service generally with 90 days' prior written notice to all Developers.
5. Upon termination: (a) Developer's access to the Service ceases immediately; (b) Developer Data will be deleted per the Privacy Policy retention schedule; (c) since Payload Data is not stored, there is no payload data to return or delete; (d) clauses 4, 8, 10, 11, 13, and 14 survive termination.

Article 13 — Confidentiality

1. Each party shall keep the other's confidential information strictly confidential and shall not disclose it to third parties without prior written consent, except as permitted by these Terms or required by law. Where PREM receives a government or law enforcement request for Developer Data, PREM will follow the procedure described in the Privacy Policy (Section 6A) before producing any Developer Data.
2. PREM's confidential information includes the Service's technical architecture (other than what is disclosed through open-source attestation), security mechanisms, unreleased features, and pricing. Developer's confidential information includes API Keys, business information shared with PREM, and any output or metadata that could reveal Developer's use of the Service.
3. Confidentiality obligations survive termination of these Terms for 5 years.

Article 14 — General Provisions

1. **Entire Agreement:** these Terms, together with the DPA, Privacy Policy, and SLA, constitute the entire agreement between the parties regarding the Service and supersede all prior discussions and agreements.
2. **Amendments:** PREM may update these Terms on 30 days' prior written notice (or immediately for security-related changes or changes required by law). Continued use after the effective date constitutes acceptance. If Developer does not accept, Developer may close the Account before the effective date.
3. **Assignment:** Developer may not assign these Terms without PREM's prior written consent. PREM may assign these Terms to any affiliate or successor entity, provided that the TEE warranty obligations in Article 4 are expressly assumed by the assignee.
4. **Severability:** if any provision is found invalid or unenforceable, it will be modified to the minimum extent necessary and the remaining provisions will remain in full force.
5. **Waiver:** failure to enforce any provision is not a waiver of that right.
6. **Force Majeure:** neither party is liable for delays caused by events beyond reasonable control, including natural disasters, government actions, or internet disruptions. Force majeure does not excuse any failure of the TEE architecture or encryption systems, which are within PREM's control.
7. **Language:** the controlling language is English. Where PREM provides translations for convenience, the English version prevails in case of conflict.

Article 15 — Governing Law and Jurisdiction

1. These Terms are governed by Swiss law, excluding its conflict of laws rules and the CISG.
2. The parties submit to the exclusive jurisdiction of the courts of the Canton of Zurich, Switzerland (Handelsgericht des Kantons Zürich as court of first instance for commercial disputes above CHF 30,000).
3. Either party may seek emergency injunctive or interim relief from any court of competent jurisdiction.
4. If Developer is a consumer in the EU/EEA, nothing in these Terms affects Developer's statutory rights under applicable EU consumer protection laws, including the right to bring proceedings in the courts of Developer's habitual residence.

Contrada di Sassello 5, 6900 Lugano, Switzerland

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

Version 1.1 · PREM SA