



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Privacy Policy

Personal data processing on the website in commercial relationships and on the platform

corePTT platform

Compliance and governance

Security and data protection

03

corePTT governance

Revision 1.3 • 14 October 2026

sales@coreptt.com

COREPTT TECNOLOGIA LTDA

CNPJ 69.599.966/0001-93 • Campinas SP

Revision 1.3 | 14 October 2026

DRAFT FOR LEGAL REVIEW

corePTT Privacy Policy

Personal data processing on the website in commercial relationships and on the platform

Legal and commercial entity	COREPTT TECNOLOGIA LTDA
CNPJ	69.599.966/0001-93
Trading name	COREPTT TECNOLOGIA
Registered address	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
City and state	Campinas/SP
CEP	13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14 October 2026
Document status	Draft for legal review

This Policy sets out the data that may be processed, its purposes, the roles of the PROVIDER and CUSTOMER, retention criteria and the means for data subjects to exercise their rights. It covers commercial relationships, portals, contracted operation and the free 7-day evaluation.

This document forms part of the corePTT documentation and must be read together with the instruments applicable to its purpose. The 7-Day Trial Agreement and activation form apply to the free trial. The documents identified in the Service Order apply to paid operation. Incorporation requires the documents to be made available before acceptance, with their title, revision and date; future changes have no automatic or retroactive contractual effect.

Identification of the PROVIDER

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered under CNPJ No. 69.599.966/0001-93, with its registered office at Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270, hereinafter the PROVIDER.

The brand used is corePTT, with core in lowercase and PTT in uppercase. The PROVIDER must be identified in commercial, tax and evaluation instruments; the brand does not replace the identification of the legal entity.

Sales and contracting: sales@coreptt.com; registered telephone: (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. Revision 1.3 dated 14 October 2026. Draft for legal review.

1 Who processes the data

COREPTT TECNOLOGIA LTDA, CNPJ 69.599.966/0001-93, with its registered office at Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270, acts as controller for its own purposes that it actually determines, such as commercial relationships, contract management, fraud prevention, security and compliance with obligations. The privacy channel is legal@coreptt.com.

The CUSTOMER defines the purposes and essential means of processing its users' data, communications and location. When the PROVIDER processes this data under the CUSTOMER's lawful, documented instructions, it will act as processor, including during the trial. For its own purposes, it may act as an independent controller. Classification depends on each specific purpose and will be documented in the DPA or evaluation instrument.

2 Who this policy applies to

This Policy covers portal visitors, customer and partner representatives, platform users, demonstration participants, support contacts and data subjects whose data is entered into a corePTT environment. It does not replace specific notices presented by the CUSTOMER in its capacity as controller.

3 Data that may be processed

Category	Examples
Professional registration	name, company, position, corporate email address, telephone and user identifier
Account and authentication	login, identifiers, authentication factors, access history and permission changes
Device and network	IP, model, operating system, application version, technical identifiers, carrier and diagnostics
Operational use	groups, channels, PTT events, presence, status, times, dispatch records and communication metadata
Content	audio, video, messages, attachments and recordings when the feature is enabled
Location	coordinates, date, time, accuracy and history, according to the CUSTOMER's configuration
Support	tickets, support recordings, evidence, logs and communications with the technical team
Commercial and tax	proposals, contracts, billing contacts, tax invoices, payments and strictly necessary banking data
Website and cookies	pages visited, consent preferences, access source and browsing data described in the Cookie Policy

Voice, video or message content may reveal sensitive information. As a rule, the platform does not require these categories. Sensitive personal data and data concerning children or adolescents are excluded from the free trial unless a specific prior agreement is made and legal requirements are met. Projects involving them must document the purpose, legal basis, necessity, safeguards, permissions and retention before activation.

4 How data is obtained

- directly from the data subject through registrations, forms, meetings, demonstrations and tickets;
- from the CUSTOMER, which creates accounts, groups, permissions and settings;
- automatically during use of the application, devices and integrations;
- from partners, resellers, manufacturers, carriers or public databases, when necessary for the commercial relationship and permitted by law.

5 Purposes and legal bases

Purpose	Usual legal basis and notes
Negotiate contract and perform services	precontractual steps and performance of a contract; legitimate interest for compatible business contacts
Create accounts and provide features	legal basis defined by the controller for the purpose and data subjects; the PROVIDER follows lawful, documented instructions when acting as processor
Provide support and maintain quality	performance of a contract; legitimate interest subject to a necessity assessment and balancing test
Protect accounts and investigate abuse	compliance with a legal obligation, lawful exercise of rights or legitimate interest where applicable, documented according to necessity, proportionality and balancing
Bill and maintain records	performance of a contract and compliance with legal, tax and accounting obligations
Send commercial communications	consent when required or legitimate interest within an existing business relationship, always with an opt-out mechanism
Respond to data subjects and authorities	compliance with a legal or regulatory obligation and lawful exercise of rights
Use nonessential cookies	consent, with the ability to refuse and withdraw

Each processing activity must have a legal basis appropriate to its purpose and the data subjects involved. Accepting an engagement or this Policy does not constitute blanket consent from users. The CUSTOMER's instructions do not replace identification of a legal basis by the controller. When consent applies, it will be specific and informed, with the ability to refuse and withdraw; withdrawal does not affect processing validly carried out before it.

6 The CUSTOMER's role as controller

The CUSTOMER must inform data subjects in advance about monitoring, recording, location, purposes, administrator access and retention; adopt an appropriate legal basis; limit permissions; and honor rights. Decisions on worker monitoring depend on necessity, proportionality and applicable law. The PROVIDER will process operational data under lawful, documented instructions and will not replace that assessment with contractual acceptance.

7 Data sharing

The PROVIDER shares data only when necessary to provide the service, meet an obligation, exercise rights or carry out a legitimate business operation. Recipients may include providers of cloud, communication, monitoring, support, signature, billing and accounting services, and manufacturers and integrators associated with the environment. Each supplier must receive only the data necessary for its role and undertake compatible confidentiality and security obligations.

Data may also be provided to a competent authority pursuant to an order or valid legal basis. Whenever permitted, the PROVIDER will assess the lawfulness and scope of the request and record its response.

8 Subprocessors

Service providers and subprocessors applicable to the environment, their role, processing countries and relevant channels must be identified in an annex or list made available to the CUSTOMER before activation. Changes will follow the DPA procedure or a written agreement. Data protection objections will be assessed and may require a feasible alternative or termination of the feature, in accordance with the applicable instruments.

9 International transfers

Data may be accessed or stored outside Brazil only when the contracted architecture uses a supplier or team abroad. The PROVIDER and CUSTOMER must identify countries, recipients and purposes in the DPA or Technical Annex and adopt a valid mechanism under Article 33 of the LGPD.

When the standard contractual clauses in CD ANPD Resolution No. 19 of 2024 are used, the official text will be incorporated in full and without amendment into the instrument signed between exporter and importer. The Policy or specific page must provide clear information on the method, duration, destination, responsibilities and channel for exercising rights.

10 Retention

Record	Retention criterion
Account data	account term and the period necessary for closure, auditing and exercise of rights
Voice video messages and location	period selected by the CUSTOMER in the Service Order, subject to a legal block or valid preservation
Application access records	statutory minimum applicable to application providers, in a controlled, secure environment, and a justified additional period
Tickets and technical evidence	time necessary for support, change history, prevention of recurrence and defense of rights
Tax and contractual data	applicable statutory, regulatory and limitation periods
Incident records	at least five years from the record, in accordance with CD ANPD Resolution No. 15 of 2024
Cookies	period indicated in the preference center or until withdrawal, where applicable
Operational trial content	deletion or anonymization within 30 days after the end; residual backups within 90 days after the end; technical validation before signature and applicable legal exceptions

Data deleted from the active environment may persist in protected backups for the cycle disclosed in the engagement, with restricted access and no operational use. During the trial, residual data will be purged within 90 days after its end, a period subject to architecture validation before signature. Retention for a legal obligation or lawful exercise of rights will have a limited purpose, restricted access and the applicable period.

11 Automated decisions

corePTT may generate alerts, technical indicators and automatic rules configured by the CUSTOMER. The PROVIDER must not use these results to independently make decisions affecting the data subject's interests. If the CUSTOMER configures an automated decision-making process, it must disclose the relevant logic and ensure the rights provided for in Article 20 of the LGPD, where applicable.

12 Security

The PROVIDER will maintain technical and administrative measures proportionate to the nature of processing and the risk, in accordance with the controls actually applicable to the environment and the commitments in the DPA or trial. The CUSTOMER and users must protect credentials, devices, networks, integrations and profiles under their responsibility. This Policy does not assert certification, independent auditing, end-to-end encryption or absence of incidents.

13 Security incidents

The party identifying an incident involving personal data will notify the other without undue delay, providing available information and updates for containment, investigation and assessment. The controller will assess and make notifications to ANPD and data subjects when required, within statutory timeframes; the processor will provide the necessary cooperation. The allocation of roles does not exclude either party's own obligations. Incidents and decisions will be recorded under the applicable provisions.

14 Data subject rights

- confirm the existence of processing and obtain access to data;
- correct incomplete, inaccurate or outdated data;
- request anonymization, blocking or deletion of unnecessary, excessive or noncompliantly processed data;
- request portability under the regulations while safeguarding trade and industrial secrets;
- obtain information on data sharing and the possibility of refusing or withdrawing consent;
- object to unlawful processing and request review of an automated decision, where applicable;
- petition ANPD and exercise rights before competent protection bodies.

Requests may be sent to legal@coreptt.com with sufficient information to locate the data and confirm identity. The PROVIDER may request proportionate verification to prevent fraud. When the CUSTOMER is controller, the request will be forwarded to the responsible party or handled under its lawful instructions, without excluding the PROVIDER's own duties. Responses will observe applicable statutory timeframes, including the complete access statement within fifteen days when required.

15 Data protection officer

The public channel for data subjects and authorities is legal@coreptt.com. The identification and professional details of the data protection officer, when required, must be published in accordance with the LGPD and applicable regulations. The officer receives communications, advises the organization and performs the relevant statutory activities. Naming the channel does not assign a role or formal appointment to an unidentified person.

16 Updates

Updates may reflect legal, technical or operational changes and will be identified by revision and date. Material changes will be communicated in a manner appropriate to the processing and existing relationship. They will not retroactively validate unlawful processing or automatically become part of an

existing contract. Policies incorporated into the contract must have been made available and identified before acceptance; changes will follow the agreed procedure and mandatory rules.

Data in external integrations

An integration must transmit only the data necessary for the contracted function. The Policy, DPA or subprocessor list must disclose supplier categories, purposes, data categories, processing location and the mechanism applicable to international transfers.

Using third-party infrastructure or software does not exclude the PROVIDER's obligations for processing under its responsibility. When a supplier acts as an independent controller, that status and the corresponding service channel must be clearly presented to the data subject.

Retention of operational content

In paid operation, recordings will be available for up to 90 calendar days on a rolling basis only when the feature and that period are contracted. Periods for messages, files, location and other content will be defined in the Service Order and DPA according to purpose, legal basis, capacity and controls. Content may be deleted at the end of the applicable period, subject to lawful preservation.

The contractual recording period does not automatically extend to registration, billing, access records, security, tickets, incidents, contractual evidence or fulfillment of rights. Each category will be retained only for the period necessary for its purpose and applicable obligations. The free trial does not guarantee retention or availability of recordings for 90 days.

Evaluation and proof-of-concept data

The standard trial lasts 7 calendar days, equivalent to 168 hours from the communicated activation. Fictitious, anonymized or minimized data should be preferred. At the end, access may be terminated without automatic conversion to a paid plan. The CUSTOMER must arrange exports before expiry. Without a contract or lawful preservation, operational content will be deleted or anonymized within 30 days after the end; residual backups will be purged within 90 days after the end, without operational reuse. These periods must be validated against the architecture before signature.

Hosting, processing countries, service providers, recording and location features, and the CUSTOMER's instructions must be disclosed and validated before trial activation. Communication content will not be used for advertising, sale to third parties or training AI models without a specific agreement and appropriate legal basis. Continuation after the trial requires formal engagement through sales@coreptt.com and does not ensure recovery of content already deleted.

Public bodies and entities remain responsible for defining the public purpose, authority, legal basis, public disclosure, information classification and internal authorizations. Data connected with public safety, national defense, State security or criminal investigations may be used in a trial only under the applicable specific legal regime and public oversight.

Backups and deletion requests

Backups serve continuity and recovery, not archiving or routine consultation. During the purge cycle, deleted content will be isolated from normal use, protected and erased through secure rotation. If a technically necessary recovery reintroduces data whose deletion was requested, the deletion instruction must be reapplied. The trial does not guarantee backup, restoration or recovery of data already deleted.

Document control

Field	Record
Documentation owner	COREPTT TECNOLOGIA LTDA
Document status	Draft for legal review
Sales channel	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com