



Push-to-talk solution

corePTT Document Guide

Company identification revision and application of the instruments

This guide identifies the revised document set, the rules aligned with the free 7-day trial agreement and the fields to be validated for each engagement. The documents are available in editable Word and PDF formats, with revision 1.3 dated October 14, 2026.

Company information

Legal name: COREPTT TECNOLOGIA LTDA

Trade name: COREPTT TECNOLOGIA

Brand: corePTT

CNPJ: 69.599.966/0001-93

Registered office: Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270.

Registered telephone number: (11) 9839-0601

Sales: sales@coreptt.com

Legal privacy and integrity: legal@coreptt.com

Main adjustments

References to the previous companies and addresses have been replaced with the identification shown in the attached CNPJ registration document. The additional address detail HR 115675 and the conflicting telephone number in the reference agreement have been corrected in accordance with the registration.

The standard trial has been aligned to 7 calendar days, equivalent to 168 hours from the notified activation. There is no automatic conversion to a paid plan, retroactive charge for the free license or purchase obligation. Continuation requires an accepted proposal and a formal engagement.

The security, privacy, use, hosting and backup policies have been harmonized with this evaluation. Commercial SLA targets and retention of recordings for up to 90 days require an express engagement and do not extend the free trial.

Documents in the set

The individual files retain their purposes. The updated trial agreement also has an editable version in addition to the PDF.

Code	Document
01	corePTT Legal Notice and Company Identification
02	corePTT Terms of Use
03	corePTT Privacy Policy
04	corePTT Cookie Policy
05	corePTT Acceptable Use Policy
06	corePTT Security and Trust
07	corePTT Business Agreement
08	corePTT Data Processing Agreement
09	corePTT Support and Availability SLA
10	corePTT Service Order and Commercial Proposal
11	corePTT Technical Annex on Features Compatibility Equipment and Testing
12	corePTT Development Customization and Integrations Annex
13	corePTT 07-Day Evaluation and Testing Agreement
14	corePTT Backup Retention and Deletion Policy
15	corePTT Hosting and Server Management Policy
CT	corePTT 07-Day Trial Agreement EN

Document 13 brings together the tables and evaluation procedure. Agreement CT governs the free license and trial clauses. If used together, both must be identified upon acceptance and have the same limits, dates and responsible persons. Any discrepancy requires a written amendment before activation.

Validation before use

Free trial

Complete the details of the CUSTOMER and its representatives, verify signing authority and identify the environment. Record the start and end with the time and Brasília time zone, limits for users, devices, groups, storage, features, integrations, and permissions for recording and location.

Provide information on providers, countries and subprocessors before activation. Where there is an international transfer, define and formalize the applicable legal mechanism. Validate access controls, notices to data subjects, legal bases, alternative communication and available support.

Confirm against the architecture the erasure or anonymization of operational content within 30 days after the end and the purge of residual backups within 90 days after the end. Records retained on a legal basis or for the lawful exercise of rights remain restricted to the applicable purpose.

Arrange exports before expiry and document any extension with a new end date. Mere contact with sales does not extend access or guarantee recovery of erased data.

Contracted operation

Select modules, quantities, prices, taxes, periods, payment terms and any expressly agreed renewal. Complete deployment, acceptance criteria, hosting, support, availability, channels and escalation, retention by category, backup, RPO and RTO where these are contractual targets.

Identify by title, version and date the documents made available before acceptance. Do not automatically incorporate future versions or retroactively change obligations. Identify the data protection officer where appointment and disclosure are required; the legal@coreptt.com channel does not imply that a specific person has been appointed.

Verified regulatory sources

Law No. 13.709/2018 LGPD, particularly processing roles, instructions, security and incidents.
[Official text on Planalto](#)

ANPD regulations and guidance on incident notification: notification by the controller where required and cooperation by the processor without undue delay.
[Official ANPD guidance on incidents](#)

CD/ANPD Resolution No. 19/2024, with the updated text and correction indicated by the ANPD, for international transfers. The DPA and its summaries do not replace formalization of the selected mechanism.
[Official ANPD international transfer regulations](#)

The drafts must undergo legal review and operational validation before signing, in accordance with the document status of the reference agreement.



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Legal Notice and Company Identification

Entity responsible for the offering nature of services and institutional limits

corePTT platform

Compliance and governance

Security and data protection

01

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 Legal Notice and Company Identification

Entity responsible for the offering nature of services and institutional limits

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 document identifies the company responsible for the corePTT offering in Brazil, its channels and the scope of services. It distinguishes the PROVIDER's obligations from the responsibilities of manufacturers, carriers and external service providers, and sets out the rules applicable to free evaluation and business contracting.

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 Identification of the responsible entity

Information	Identification
Legal and commercial entity	COREPTT TECNOLOGIA LTDA
CNPJ	69.599.966/0001-93
Brand and platform	corePTT
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Corporate website	https://coreptt.com
Administrative console	https://admin.coreptt.com
Legal and privacy channel	legal@coreptt.com
Sales and contracting	sales@coreptt.com (11) 9839-0601

corePTT identifies the brand and platform offered by COREPTT TECNOLOGIA LTDA, CNPJ 69.599.966/0001-93, hereinafter the PROVIDER. The brand has no separate legal personality. Contracts, tax documents, billing and formal communications must identify the PROVIDER and the corresponding engagement.

2 What the offering includes

The offering may include voice communication software over IP networks, dispatch, operational groups, location, recording, video, messages, files, APIs, integrations, implementation services, support, devices and connectivity. Only the items described in the Service Order or Technical Annex form part of the contracted scope.

The terms PoC, PTTtoC, PTT, MCPTT and MCX indicate functional categories or market references. Their use does not, by itself, demonstrate compliance with 3GPP standards, certification, regulatory approval, end-to-end encryption, universal interoperability or suitability for mission-critical use. Any such commitment requires an express specification of scope and relevant technical evidence.

3 Activities of the PROVIDER

The PROVIDER may act as a reseller, distributor, integrator, implementer, support provider and commercial administrator of the solution. It is responsible for the obligations it expressly undertakes, but does not represent itself as the original manufacturer of all software, equipment, SIM cards, operating systems, mobile networks or cloud services used.

Third-party components remain subject to the specifications, licenses, lifecycles, warranties and limitations of their respective owners or manufacturers. The PROVIDER will disclose relevant known dependencies for the contracted scope.

4 Connectivity and telecommunications

corePTT is an application that uses telecommunications networks and internet access. When the PROVIDER acts as an intermediary for SIM cards, plans or connectivity, the authorized

telecommunications provider and applicable commercial conditions must be stated in the Service Order. Network coverage, capacity and continuity fall within the technical responsibility of the carrier concerned.

Unless a specific regulatory engagement is agreed, the platform is treated as a value-added service and does not replace the telecommunications service supporting it, pursuant to Article 61 of Law No. 9.472 of 1997.

5 Operational use and emergencies

The service does not replace the public emergency telephone service, official public safety networks or certified mission-critical systems. The CUSTOMER must maintain alternative means of communication appropriate to the risks of its activity. A project may be advertised as an emergency or mission-critical solution only if the Service Order specifies architecture, redundancy, service levels and acceptance criteria designed for that use.

6 Published information

The PROVIDER seeks to keep the corporate and technical information it publishes accurate. Demonstrations, presentations and images may show optional features or specific configurations. The scope actually enabled must be stated in the proposal, Service Order, Technical Annex or, for the free trial, the accepted activation form. Contractual documentation does not exclude binding offers or rights established by mandatory rules.

7 Intellectual property

Texts, visual identity, proprietary documentation, interfaces, compilations and other content identified as corePTT are protected by applicable law and belong to their respective owners. Third-party brands, software, libraries and equipment remain subject to their rights and licenses. No publication transfers intellectual property rights to a visitor or the CUSTOMER.

8 Data protection

Personal data processing is described in the Privacy Policy and applicable DPA. The PROVIDER acts as controller for its own purposes that it actually determines, such as sales and contract management, security and fraud prevention; and as processor for user, communication and location data processed under the CUSTOMER's lawful, documented instructions. Roles depend on the specific purpose, including during the free trial.

9 Channels and formal communications

Sales and contracting: sales@coreptt.com; registered telephone: (11) 9839-0601. Legal, privacy, data subject requests and integrity: legal@coreptt.com. Technical tickets will use the channel defined in the engagement; during the trial, sales@coreptt.com will initially route requests to the responsible team. Formal communications must comply with the contacts and requirements of the accepted instrument.

10 Applicable law

This notice is interpreted in accordance with Brazilian law, including the Lei Geral de Proteção de Dados Pessoais, Marco Civil da Internet, Lei de Software, Código Civil and Lei Geral de Telecomunicações, insofar as each rule applies to the specific case.

Solution development and integrations

corePTT may combine proprietary modules, configurations, dashboards, APIs, gateways, connectors and integration routines developed or adapted by the PROVIDER, alongside licensed components, libraries, operating systems, networks, equipment and services supplied by third parties. Commercial documentation must distinguish native features, integrated components and resold items.

The PROVIDER is responsible for the integration, configuration and support work it undertakes within the contracted scope. It does not control unilateral third-party changes, such as changes to or discontinuation of APIs, firmware, licenses, networks, operating systems or cloud services. This limitation does not exclude liability for its own acts, inappropriate selection or configuration, breach of contract or obligations that cannot legally be excluded.

Professional services customization and infrastructure

The PROVIDER offers technical discovery, development, integration, configuration, screen and workflow customization, automation, migration, implementation and assisted operation services. Each deliverable depends on requirements gathering, feasibility analysis, a proposal, a schedule, acceptance criteria and responsibilities defined in writing.

corePTT may run on shared infrastructure, with logical segregation between CUSTOMERS, or in a dedicated environment when requested and contracted. The PROVIDER manages the servers and technical layers it undertakes within the scope, without replacing the obligations of the cloud provider, connectivity carrier or CUSTOMER for resources maintained by them.

Evaluation retention and deletion

The standard free trial lasts 7 calendar days, equivalent to 168 hours counted from activation and communication of access details to the CUSTOMER, in accordance with the validated activation form. The trial license costs R\$ 0,00 and is intended for controlled evaluation; it does not include a commercial SLA, continuous availability or exclusive reliance in emergencies and critical processes. The CUSTOMER remains responsible for its infrastructure, internet access and equipment; additional items require a specific agreement.

At the end of the 168 hours, the license expires and access may be suspended. There is no automatic renewal, automatic paid conversion, retroactive trial charge or purchase obligation. Continuation requires an accepted proposal and formal engagement through sales@coreptt.com; contacting sales does not extend the period or guarantee preservation of data. A free extension may be granted only in writing, with a new end date.

In paid operation, recording retention for up to 90 calendar days on a rolling basis applies only when the feature and period are expressly contracted. Other content categories, longer retention, historical archiving and restoration are governed by the Service Order, DPA and Backup Policy, with an appropriate purpose and legal basis. The free trial does not guarantee recording availability for 90 days.

Before the end of the trial, the CUSTOMER must request or perform the necessary exports. Without a contract or lawful preservation, operational trial content will be deleted or anonymized within 30 days after the end, and residual backups within 90 days after the end, without operational reuse. These periods must be validated against the architecture before signature. Retention required by law or for the lawful exercise of rights will have a limited purpose and restricted access.

corePTT brand and third-party brands

The institutional spelling is corePTT. The name, logo, visual identity, domains, documentation and proprietary components are protected by applicable law. The expression registered trademark and the ®

symbol may be used only after valid registration is granted by INPI and with correct identification of the owner and registration number.

Hytera, Caltta, Motorola Solutions, MOTOTRBO, WAVE PTX, HyTalk, eChat and other brands mentioned belong to their respective owners. References are intended to identify them and describe interoperability. Tests or integrations conducted by the PROVIDER do not represent manufacturer certification, endorsement, association, exclusive representation or partnership unless formally documented.

© 2026 COREPTT TECNOLOGIA LTDA. All rights reserved to their respective owners. Content from manufacturers, standards and third parties remains subject to applicable rights and conditions.

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



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Terms of Use

Rules for business access to the platform and applications

corePTT platform

Compliance and governance

Security and data protection

02

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 Terms of Use

Rules for business access to the platform and applications

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

These Terms govern the daily use of corePTT by administrators and end users, including accounts, recording, location, integrations, connectivity, support and termination.

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 Acceptance and scope of application

These Terms govern access to corePTT portals, applications, consoles, APIs and features. Their version and the applicable policies must be made available before acceptance, identifying the title, revision and date. Acceptance will be recorded by the agreed method; merely receiving credentials or installing the application does not replace the authority to represent the organization required for business contracting, nor does it constitute blanket consent to data processing.

When access arises from a contract between the PROVIDER and an organization, the user will act under that organization's authorization. For paid operation, the Service Order and Business Agreement govern the commercial relationship, the DPA governs processing under the CUSTOMER's instructions and the SLA governs service levels. During the trial, the 7-Day Free Trial Agreement and validated activation form prevail, without incorporating unaccepted commercial conditions. Discrepancies require a written agreement, subject to mandatory rules.

2 Who may use the platform

The platform is intended for organizations and persons authorized by them, with legal capacity and a valid relationship or authorization. corePTT is not directed at children or adolescents. Their data and sensitive personal data are excluded from the free trial unless a specific prior agreement is made, the legal basis is defined and applicable requirements and safeguards are met.

3 Account and credentials

Each account is personal and must correspond to an identifiable user. Credentials must not be shared, transferred or retained on devices without appropriate protection. The user must report loss of a device, suspected unauthorized access or a change in their employment or work relationship as soon as they become aware of it.

The administrator designated by the CUSTOMER may create, change, suspend and delete accounts, groups and permissions. The PROVIDER may perform these actions on the administrator's instructions or to contain a security risk, comply with the law or prevent use contrary to the contractual documents.

4 License to use

During the term of the engagement or trial and within the enabled limits, the PROVIDER grants a limited, nonexclusive, nontransferable license for the CUSTOMER's internal activities. Suspension and termination will follow the circumstances set out in the accepted instrument. The license does not include source code, technology transfer, sublicensing rights or components that have not been contracted.

5 Available features

Features vary according to the plan, version, device, integration, network and permissions. For paid operation, the scope must be stated in the Service Order or Technical Annex; for the trial, in the activation form validated before the start. The presence of a button or documentation reference does not by itself enable a feature outside the scope, subject to rights arising from a binding offer and mandatory rules.

6 User obligations

- use the platform only for authorized, lawful professional purposes;
- follow the CUSTOMER's internal rules on recording, location, confidentiality and security;
- keep the application, operating system and device on supported versions;
- respect third-party rights and the restrictions in the Acceptable Use Policy;
- provide accurate information when opening a ticket or requesting assistance;
- stop using the service and contact the appropriate channel upon detecting a risk to people, data or operations.

7 Administration by the CUSTOMER

The CUSTOMER defines purposes and legal bases, designates users and groups, and decides on recording, location and retention within the enabled scope. It must inform data subjects in advance, limit access and observe necessity, proportionality, labor, privacy and confidentiality rules. These decisions do

not replace technical limitations and accepted periods; acceptance of the Terms does not constitute blanket consent from users.

8 Communications and recordings

Voice, video, messages and files may be transmitted, recorded and accessed only through enabled features and by authorized profiles. The CUSTOMER must inform users in advance about recording and administrative access; interface indicators supplement this information and do not replace it. Content remains protected by confidentiality, purpose limitation and necessity, including in relation to the administrator.

9 Location

The location feature depends on device permissions and the availability of satellites, networks and sensors. Data may be delayed, have a margin of error or be unavailable. The CUSTOMER must define the purpose, legal basis, access profiles and retention before enabling the feature. Location must not be used as the sole basis for a decision that may affect the user's physical safety or rights.

10 Integrations and devices

Integrations with radios, smartphones, dispatch systems, DMR, APIs, third-party platforms or accessories depend on compatible models and versions. Changes made by the manufacturer, carrier or integration supplier may require an update, reconfiguration or component replacement.

11 Connectivity

Service performance depends on the network used by the user. Areas without coverage, congestion, data allowance limits, firewall restrictions, battery saving, roaming and carrier quality policies may affect calls and data. The CUSTOMER must maintain connectivity suitable for its operation and alternative means for critical activities.

12 Updates and technical changes

The PROVIDER may correct defects, update interfaces and components, and discontinue versions for security, compatibility or lifecycle reasons. Material changes reducing a contracted feature require notification and the treatment provided for in the contract; changes in scope must be documented. Urgent measures may be taken without prior notice to contain a risk or comply with the law, with subsequent notification when permitted. A third party's decision does not exclude responsibility for the PROVIDER's own conduct.

13 Maintenance

Scheduled maintenance will be communicated in accordance with the contracted SLA. Emergency interventions may take place without prior notice to contain a vulnerability, preserve data or restore service. The free trial does not include a commercial SLA; foreseeable impacts will be communicated where possible, and any extension requires a written agreement with a new end date.

14 Support

Tickets must specify the environment, problem, time, impact, available evidence and responsible contact. For paid operation, the channel and timeframes will follow the contracted SLA; an initial response is not equivalent to a resolution. During the trial, initial support must be requested through sales@coreptt.com for

routing to the responsible team, subject to availability and the agreed scope, without a commitment to 24-hour support.

15 Privacy

The Privacy Policy describes the PROVIDER's own processing as controller and processing under the CUSTOMER's instructions as processor. For user, communication and location data whose purposes are defined by the CUSTOMER, the DPA or the trial's data provisions apply. Requests may be sent to legal@coreptt.com, with cooperation from the administrator or person responsible for processing at the CUSTOMER.

16 Ownership of data and content

The CUSTOMER retains its rights over content it enters into the platform and declares that it has authorization to process it. It grants the PROVIDER limited permission to host, transmit, make technical copies of, recover, protect and make that content available to the extent necessary to provide the service and comply with the law.

17 Ownership of the platform

The platform, its documentation, brands, routines, interfaces and improvements belong to the PROVIDER or their respective licensors. Comments and suggestions may be used to improve the service without transferring the CUSTOMER's confidential content or intellectual property to the PROVIDER.

18 Suspension of access

The PROVIDER may suspend an account when there is a security risk, an order from an authority, payment default provided for in the contract, unlawful use or a material breach of these Terms. Whenever circumstances permit, the CUSTOMER will be informed and given an opportunity to remedy the cause. Urgent measures may be taken immediately to limit damage.

19 Service limitations

The PROVIDER does not guarantee uninterrupted communication at every location, absolute GPS accuracy, compatibility with every device or complete absence of failures. Warranties, service levels and contractual remedies are those provided in the Business Agreement and SLA, subject to rules that do not permit limitations.

20 Termination and export

At the end, access will be terminated in accordance with the accepted instrument. The CUSTOMER must request or perform exports it wishes to retain before termination, using the available formats and features. During the trial, there is no right to subsequent access, guaranteed recovery or retention of recordings for 90 days. Deletion, backup and legal preservation periods will follow the specific trial provisions and Backup Policy.

21 Changes law and disputes

This version is identified by revision and date. External policies will form part of the engagement only if made available before acceptance and identified by title, version and date. Future changes will not be incorporated automatically or have retroactive contractual effect; material changes will follow the agreed procedure. Brazilian laws and mandatory rights apply. The parties will seek an agreed resolution; the forum will be that provided for in the accepted instrument, subject to mandatory statutory jurisdiction.

22 Trials demonstrations and experimental features

Proofs of concept, demonstrations, preliminary versions and beta features are intended for controlled evaluation and may have limited capacity, support and availability. The standard trial lasts 7 calendar days, equivalent to 168 hours from the communicated activation. The form must specify limits, features, recording, location, hosting, countries and service providers before the start. Features not enabled are outside the scope; changes require a written record.

23 Communications and records

Operational notices may be sent through the application, portal or registered contacts. Authentication, acceptance, administrative change and support records may be used for security, contract performance and the lawful exercise of rights, subject to the Privacy Policy, DPA and applicable periods. The CUSTOMER must keep its contact details up to date.

24 Contact

Sales and contracting: sales@coreptt.com; registered telephone: (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. For paid operation, technical tickets will use the plan's channel; during the trial, sales will perform initial routing. The legal channel does not replace opening a technical ticket or contacting the public emergency service.

Third-party applications and components

Integrated features may depend on third-party applications, APIs, maps, application stores, operating systems, mobile networks, cloud services, equipment or licenses. These components are also subject to their suppliers' terms and policies.

The PROVIDER remains responsible for the components and services it supplies directly. Failures caused exclusively by a third party and outside its reasonable control will be handled in accordance with the contract and SLA, with initial diagnosis and escalation when the contracted plan includes that activity.

Professional services and on-demand changes

Integrations, solution development, customization, imports, reports, dashboards, business rules and visual adaptations may be contracted separately. Requests will undergo impact analysis, estimation, prioritization, commercial approval and acceptance. Making a customization available does not mean it will be included in all versions or plans.

Shared and dedicated environments

In a shared environment, computing resources may be used by more than one CUSTOMER, with logical segregation controls. In a dedicated environment, the resources identified in the Service Order are reserved for the CUSTOMER; the provider's networks, control services or physical infrastructure may still be shared unless additional isolation is expressly committed to.

Free 7-day evaluation

The trial license costs R\$ 0,00 and ends after 168 hours from activation and communication of access details. Access may be suspended, including access to dispatch, location and recordings. There is no automatic renewal or conversion to a paid plan, retroactive charge for the free license or purchase obligation. A free extension requires written authorization and a new end date. The CUSTOMER must maintain contingency arrangements and must not rely exclusively on the trial for life safety, emergencies or critical processes.

To continue, the CUSTOMER must contact sales@coreptt.com and formalize an accepted proposal and engagement setting out prices, licenses, support, service levels and data processing. Contact does not extend the trial or guarantee data recovery. Without a contract or lawful preservation, operational trial 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. Legal retention will be restricted to the applicable purpose.

Standard operational retention

In paid operation, recordings may remain available for up to 90 days on a rolling basis when the feature and period are contracted. Messages, files, location and other categories will have the periods defined in the Service Order and DPA. Longer retention or historical archiving depends on feasibility, purpose, legal basis and express agreement. The free evaluation follows its own provisions and does not guarantee recordings for 90 days.

Users and administrators must protect credentials, data, settings and nonpublic documentation, restricting access to the necessary persons. Fraud, improper benefits, concealed conflicts of interest and use of the trial to circumvent authorization levels or purchasing procedures are prohibited. Irregularities may be reported to legal@coreptt.com, with restricted handling and no retaliation for good-faith reporting. The duration of confidentiality and audit rights follow the accepted instrument; an audit does not grant unrestricted access to infrastructure, third-party data or source code.

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



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



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Cookie Policy

Cookies preferences and consent on corePTT portals

corePTT platform

Compliance and governance
Security and data protection

04

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 Cookie Policy

Cookies preferences and consent on corePTT portals

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

This Policy distinguishes necessary technologies from optional ones and defines how visitors can accept, reject or change their choices without losing access to essential functions.

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

Identification of the PROVIDER

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with the CNPJ under 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 letters and PTT in uppercase letters. The PROVIDER must be identified in the commercial, tax and evaluation instruments; the brand does not replace identification of the legal entity.

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

1 Purpose

This Policy explains how corePTT portals use cookies and equivalent technologies, such as local storage, pixels and identifiers. It must be read together with the Privacy Policy and the options displayed in the preference center.

2 What cookies are

Cookies are small files or records saved in the browser or on the device. They can maintain a session, remember choices, measure use or enable third-party content. Session cookies expire at the end of browsing; persistent cookies remain for the period specified in the inventory or until they are deleted.

3 Categories used

Category	Purpose	Rule
Strictly necessary	authentication, security, load balancing, consent and requested functionality	active for technical reasons; not used for advertising
Preferences	remember the user's language, display and choices	require consent when not necessary for the requested service
Measurement and performance	understand aggregate use, failures and page performance	remain disabled until consent is obtained when they identify or may single out the visitor
Communication and advertising	measure campaigns, limit repetition and personalize communication	only after specific consent; must not be a condition for access to essential content
Third-party content	load a video, map, chat or other embedded feature	enabled according to the user's choice and the need for the feature

4 Legal basis

Necessary cookies will be limited to the requested functions and relevant security controls, with the legal basis assessed for the specific purpose. Unnecessary technologies for individualized measurement, optional preferences, advertising and third-party content will remain blocked until valid consent is obtained, where applicable. Acceptance of the contract or this Policy does not constitute general authorization for tracking.

5 Consent panel

On the first visit, the portal must provide a clear option to accept, reject or configure unnecessary cookies. Rejecting them must be as simple as accepting them. Optional categories cannot be preselected. The choice will be recorded and may be changed at any time through the preferences link available in the footer.

6 Current inventory

The inventory made available to visitors must identify, for each active technology, its name, supplier, domain, purpose, category and duration. The PROVIDER must technically validate this inventory before publication and whenever relevant changes occur. New purposes and optional technologies require prior information and, where applicable, a new choice by the visitor. The inventory does not automatically incorporate future obligations into the business agreement.

7 Third-party cookies

Suppliers of embedded content or measurement services may use their own cookies. The PROVIDER must identify the third party, purpose, period and relevant processing in the inventory and block optional

loading until a valid choice has been made. The third party's notice does not relieve the PROVIDER of its obligations regarding the selection, configuration, transparency and transfers under its responsibility.

8 How to withdraw consent

Visitors may reopen the preference center and disable optional categories. They may also delete cookies in their browser settings. Withdrawal does not affect processing lawfully performed before the change and may require reauthentication or a reset of preferences.

9 Browser signals

When a recognized and compatible technical standard exists, the PROVIDER may interpret global privacy signals as an expression of objection or preference. Until there is technical and legal uniformity, the consent panel will remain the main mechanism.

10 Retention

The duration of each cookie will be stated in the inventory. The record of the user's choice will be kept for the period necessary to demonstrate the preference and will be renewed at reasonable intervals or when the purpose changes. Data derived from measurement will not be retained for longer than necessary for the stated analysis.

11 Contact

Questions, data subject requests and privacy matters: legal@coreptt.com. The Privacy Policy contains information on rights, recipients, international transfers and the responsible channel. Sales and contracting: sales@coreptt.com; registered telephone: (11) 9839-0601.

12 Implementation reference

Configuration of the banner and inventory must follow the LGPD principles of purpose, necessity, transparency, prevention and non-discrimination and the recommendations of the Guidance on Cookies and Personal Data Protection published by the ANPD.

External technology suppliers

Third-party cookies or equivalent technologies must only be enabled in accordance with the category, purpose and legal basis specified in the current inventory. The PROVIDER does not claim to control those suppliers' own policies, but is responsible for the selection, configuration and transparency of the tools it incorporates into its environments.

Temporary evaluation portals

Portals for the free 7-day trial, equivalent to 168 hours from the notified activation, follow this Policy. The end of the trial terminates access in accordance with the evaluation instrument, without automatic renewal or automatic conversion to a paid service. Environment identifiers will be deleted according to their purpose; records needed to demonstrate choices, prevent abuse or meet an obligation may be retained for a justified period. The trial's operational content and residual backups are subject to the limits of 30 and 90 days after the end of the trial, subject to validation of the architecture before signature.

This revision must be made available before any contractual incorporation and identified by title, version and date. Policy changes will not be automatically incorporated into existing instruments or validate retroactive processing; the amendment procedure and data subjects' rights must be observed.

Document control

Field	Record
Entity responsible for documentation	COREPTT TECNOLOGIA LTDA
Document status	Draft for legal review
Sales channel	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com

corePTT Acceptable Use Policy

Permitted conduct restrictions and response to misuse

corePTT platform

Compliance and governance
Security and data protection

05

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 Acceptable Use Policy

Permitted conduct restrictions and response to misuse

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

This Policy establishes practical rules for communication, recording, location tracking, APIs, devices and security. It applies to contracted operations and the free 7-day evaluation, subject to the features, limits, purposes and responsibilities documented in each instrument.

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

Identification of the PROVIDER

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with the CNPJ under 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 letters and PTT in uppercase letters. The PROVIDER must be identified in the commercial, tax and evaluation instruments; the brand does not replace identification of the legal entity.

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

1 Purpose

This Policy protects people, networks, devices, customers and the platform itself. It applies to users, administrators, integrations, APIs, connected applications and anyone who uses a corePTT credential or resource.

2 Authorized use

The service must be used for legitimate professional communication, within the scope approved by the CUSTOMER and the permissions assigned. Users may not bypass controls, exploit a function for an undisclosed purpose or use another organization's environment without authorization.

3 Prohibited content and conduct

- threats, stalking, harassment, discrimination, exploitation, extortion or incitement to violence;
- unlawful, fraudulent or defamatory material, or material that violates confidentiality, image rights, intellectual property or privacy;
- use to coordinate crime, obstruct authorities or conceal illegal activity;
- recording, filming or locating a person without a legal basis and adequate information;
- disclosure of credentials, personal data or confidential information beyond operational need;
- deliberately false communication that may compromise security, continuity or incident response.

4 Security and integrity

- do not conduct load, penetration or security tests, scanning, traffic interception, vulnerability exploitation or attempts to access other environments without specific written authorization;
- do not introduce malware, destructive code, abusive automation or persistence mechanisms;
- do not bypass authentication, limits, audit logging, license restrictions or administrative controls;
- do not use a generic account when the environment requires individual traceability;
- do not connect a compromised device, a device with its protections removed or an unsupported version when this increases risk.

5 Use of APIs and integrations

Integrations must comply with the documentation, call limits, credential scope and authorized environment. Extraction without a legitimate purpose and authorization, reidentification of anonymized data, unauthorized replication or resale of the service and copies without compatible controls are prohibited. Keys and secrets must be protected and replaced if exposed; APIs not enabled within the scope are outside the trial.

6 Privacy and monitoring

The CUSTOMER must configure recording and location tracking proportionately to the stated purpose. Using corePTT for covert surveillance, discriminatory profiling, control of private life or exclusively automated decision-making without the safeguards required by law is prohibited. Access to operational content must follow functional need and audit logging requirements.

7 Use in critical environments

Users must maintain alternative means and must not rely exclusively on corePTT for assistance or command whose failure could cause death, serious injury, environmental harm or significant material loss. Any commercial commitment for critical use requires a specific project, tests, redundancy, contingency planning and formal acceptance supported by technical evidence. In the free trial, use as an emergency system or mission-critical infrastructure is outside the scope. The platform does not replace public emergency services.

8 Network resources

Causing disproportionate load, unauthorized automated calls, mass transmissions, interference, identity fraud, source masking or use that degrades other customers' experience is prohibited. The PROVIDER may apply reasonable technical limits to preserve security and availability.

9 Equipment and serial numbers

Devices supplied under rental or loan-for-use arrangements must be used at the agreed location, for the agreed purpose and in the agreed configuration. The CUSTOMER may not remove asset identification, alter firmware without authorization, break a seal or transfer equipment to a third party outside the contract.

10 Responsible vulnerability reporting

Suspected vulnerabilities must be reported confidentially to legal@coreptt.com, with a description, minimized evidence and a secure contact method. Reporting does not authorize access to third-party data, persistence, disruption or invasive testing, nor does it create an automatic reward. Any tests require written authorization specifying scope, time window and responsibilities; disclosure must respect rights, confidentiality and security.

11 Investigation

The PROVIDER may preserve relevant records, limit access and request information necessary to investigate a violation. It will consider severity, recurrence, impact and cooperation, and restrict measures to what is necessary. Processing evidence must comply with purpose, legal basis, restricted access and a justified retention period, without authorizing indiscriminate surveillance of content.

12 Consequences

A violation may result in guidance, blocking, replacement of credentials, suspension or termination, depending on severity, risk, law and the contract. The PROVIDER will state the reason where permitted and offer an opportunity to correct the situation where compatible with the risk. Urgent measures may be immediate. Communications to authorities or third parties require a legal basis and proportionate scope; the free nature of the service does not remove duties of good faith, security and data protection.

13 CUSTOMER responsibility

The CUSTOMER must train users, keep administrators up to date, review access, disable accounts of people who are no longer affiliated and investigate misuse under its control. It must cooperate with the PROVIDER in containing incidents and must not instruct users to violate this Policy.

14 Questions and exceptions

Operational exceptions require written approval from the PROVIDER and the CUSTOMER's authorized representative, specifying scope, period, risks and controls. They may not authorize unlawful conduct or waive mandatory rules. Failure to respond does not mean authorization. Changes to features and trial duration must be recorded, and contacting sales does not extend access.

Third-party rights and authorized integrations

Users may not bypass licenses, copy software, use a trademark or logo without authorization, extract code, manipulate firmware, create unapproved integrations or violate the terms of manufacturers and suppliers connected to the environment.

Use of evaluation environments

The standard trial lasts 7 calendar days, equivalent to 168 hours from the notified activation, with a license fee of R\$ 0,00 and a scope validated in the activation schedule. It does not include a commercial SLA or continuous availability. Use for emergencies, critical production, unlawful surveillance, processing outside the authorized purpose or circumvention of licenses, security and contracting procedures is prohibited. Sensitive data and data relating to children or adolescents are excluded, unless there is a prior specific agreement and the legal requirements are met.

The CUSTOMER must favor fictitious, anonymized or minimized data and arrange its exports before the trial ends. There is no automatic renewal or automatic conversion to a paid service, purchase obligation or retroactive charge for the free license. To continue, the CUSTOMER must formalize a contract through sales@coreptt.com; registered telephone: (11) 9839-0601. Without a contract or lawful preservation, operational content will be deleted or anonymized within 30 days after the end of the trial and residual backups will be purged within 90 days after the end of the trial, without operational reuse; these periods are subject to validation of the architecture before signature. The trial does not guarantee restoration or recordings for 90 days.

Public bodies and companies must internally authorize the trial, appoint a responsible person and permit only data compatible with the purpose and information classification. The parties will comply with applicable integrity and anti-corruption legislation, without undue advantage, fraud or unlawful favoritism. Approvals, scope changes and extensions will be documented. Reports of irregularities may be sent to legal@coreptt.com, with a restricted investigation and a prohibition on retaliation for good-faith conduct.

This revision and the other policies will only form part of the agreement if they are made available before acceptance and identified by title, version and date. New versions will not be automatically incorporated or retroactively amend obligations. This Policy does not assert certifications, audits or technical compliance that have not been demonstrated.

Document control

Field	Record
Entity responsible for documentation	COREPTT TECNOLOGIA LTDA
Document status	Draft for legal review
Sales channel	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Security and Trust

Governance controls shared responsibility and incidents

corePTT platform

Compliance and governance
Security and data protection

06

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 Security and Trust

Governance controls shared responsibility and incidents

Responsible provider	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Sales and contracting	sales@coreptt.com
Registered telephone	(11) 9839-0601
Legal matters privacy and integrity	legal@coreptt.com
Brand and platform	corePTT
Revision	1.3
Revision date	14 October 2026

This document presents verifiable security commitments and distinguishes the controls of the PROVIDER, the CUSTOMER, users, telecommunications operators and suppliers.

This document establishes the security controls and responsibilities for corePTT, coordinated with the Terms of Use, Privacy Policy, Acceptable Use Policy and, where contracted, the Order, Business Agreement, DPA and SLA. The free evaluation follows the 7-day agreement and does not automatically receive commercial production targets.

External documents only form part of the relationship if they are made available to the CUSTOMER before acceptance and identified by title, version and date. Future policies will not be automatically incorporated, and no revision will retroactively amend a contract; contractual changes require a written amendment accepted by the parties, subject to mandatory rules.

Identification of the provider

The PROVIDER is COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with the CNPJ under 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.

Sales and contracting: sales@coreptt.com. Registered telephone: (11) 9839-0601. Legal matters, privacy, integrity and security: legal@coreptt.com.

The PROVIDER is the legal entity responsible for the commitments it undertakes in the corePTT instruments. The CUSTOMER and representatives of both parties will be identified in the applicable instrument, with authority to approve the scope and sign.

1 Scope and transparency

This document describes the expected security model for the corePTT offering. It must not be interpreted as a certificate, audit report or guarantee that no incidents will occur. The published version must correspond to the controls actually implemented and the evidence that the PROVIDER can present under confidentiality.

2 Shared responsibility

Responsible party	Main obligations
PROVIDER	protect components under its administration, manage internal access, respond to incidents and supervise suppliers
CUSTOMER	define users, groups, permissions, retention, authorized devices and internal recording and location tracking rules
User	protect credentials and the device, install updates, follow guidance and report suspicions
Telecommunications operator and suppliers	meet their network, infrastructure, product, support and security obligations under their own contract

3 Governance

The PROVIDER must maintain designated persons responsible for security, privacy, operations and incident response; an inventory of relevant assets; periodic risk assessments; supplier acceptance criteria; change rules; and records that demonstrate the decisions taken. Exceptions must have an owner, justification, time limit and compensating control.

4 Identity and access

Administrative accounts must be individual, granted with the least privilege necessary and reviewed periodically. Multifactor authentication must be required for administrative functions whenever the component supports the feature. Credentials, keys and secrets must not be stored in plaintext or shared through inappropriate channels.

5 Environments and changes

Development, test and production environments must be separated according to the architecture. Real personal data must not be used in testing unless there is a documented need and equivalent protection. Relevant changes must have a request, assessment, approval, test, rollback plan and record appropriate to the risk.

6 Protection of data in transit and storage

The Technical Annex must identify transport protocols, available encryption, key management, storage regions and exceptions. The PROVIDER does not claim end-to-end encryption when servers need to process, record, transcode or distribute communications. The CUSTOMER will receive a sufficient description to understand this design before enabling recordings or high-risk data.

7 Records and monitoring

Administrative events, authentications, permission changes and critical actions must generate records proportionate to the risk. Access to logs is restricted, and their retention follows the security purpose, the Marco Civil da Internet, the DPA and the Service Order. Monitoring does not authorize indiscriminate surveillance of workers or content.

8 Vulnerabilities and updates

The PROVIDER must monitor vulnerabilities affecting components under its management, prioritize fixes according to criticality and exploitation risk, and maintain a process for emergency updates. Unsupported components must be replaced, isolated or protected by a documented compensating control.

9 Development and integrations

Software changes must undergo an appropriate review, dependency control and testing. APIs must require authentication, restrict scope and apply limits against abuse. Integrations supplied by the CUSTOMER must be assessed before receiving access to high-impact data or functions.

10 Backups and continuity

Backup frequency, retention period, region, restoration tests, recovery point objective and recovery time objective must be stated in the Technical Annex when they constitute contractual commitments. A backup is not a permanent archive and does not replace export by the CUSTOMER.

11 Suppliers

Suppliers with access to data or infrastructure must be assessed according to criticality and undertake confidentiality, security, incident, deletion and cooperation obligations. The PROVIDER must maintain the list of subprocessors and verify that international transfers have a valid mechanism.

12 People and confidentiality

Employees and service providers with access must be bound by a duty of confidentiality, receive guidance appropriate to their role and lose access when the need ends. Exceptional support access must be authorized, limited in time and recorded whenever the architecture permits.

13 Incident response

The process will include receipt of the alert, classification, preservation of evidence, containment, eradication, recovery, impact analysis and lessons learned. The PROVIDER, as processor of the CUSTOMER's data, will notify the controller of identified incidents without undue delay, with the available information and updates, without waiting for the investigation to end. The controller will assess and make notifications to the ANPD and data subjects when required, within the statutory periods. Each party retains its own obligations. Records of incidents involving personal data will follow the statutory retention period, including five years where applicable, in accordance with the LGPD and Resolution CD ANPD No. 15 of 2024.

14 Evidence and audits

Upon reasonable request and a confidentiality undertaking, the PROVIDER may supply completed questionnaires, architecture descriptions, policies, test reports or other available evidence. Delivery must protect trade secrets, other customers' security and information that increases the risk of attack.

15 Certifications and statements

ISO certifications, audit reports, approvals and technical compliance, including 3GPP standards, may only be advertised or contracted with valid evidence, a defined scope and a current validity period. This document does not claim certification or an independent audit. Functional compatibility and product development are not equivalent to certification.

16 Assets media and disposal

Assets that store or process information must have an owner, classification and lifecycle appropriate to the risk. Return, reuse, sale or disposal of equipment or media must include secure data removal, verification of the result and a record when criticality warrants it. The CUSTOMER's devices remain subject to its internal rules.

17 Physical infrastructure and providers

Physical controls of data centers, telecommunications and third-party facilities follow the responsibility and evidence of the respective provider. The PROVIDER must assess these controls according to criticality and must not advertise a location, redundancy, certification or surveillance that it cannot demonstrate. Facilities under direct management must restrict and record access in a manner appropriate to the risk.

18 Resilience tests

Continuity, backup restoration and incident response plans must be exercised at intervals proportionate to the risk. Results, gaps and persons responsible for corrections must be recorded. RTO, RPO, alternative region and test frequency only constitute a contractual commitment when stated in the Order or Technical Annex.

19 Review and indicators

The PROVIDER must review this document and the set of controls following a relevant change, a material incident or, at a minimum, within an internally defined periodic cycle. The analysis may consider privileged access, vulnerabilities, restorations, suppliers, incidents, exceptions and remediation plans, without disclosing information that increases the risk of attack.

20 Security contact

Security alerts and responsible vulnerability reports may be sent to legal@coreptt.com. Information about ongoing incidents must be treated confidentially to avoid compromising containment, investigation or third parties.

Supplier chain security

The PROVIDER assesses relevant infrastructure, software, API and equipment dependencies according to risk and the contracted scope. Changes of supplier or subprocessor that affect security, privacy or continuity must follow the contractual process and the DPA.

The Security and Trust page describes practices and controls, but must not claim certification, an independent audit or full compliance with a standard that has not been formally obtained and maintained.

Segregation in shared infrastructure

Shared environments must adopt logical segregation of accounts, profiles, data and permissions compatible with the validated architecture. Computing, storage, network and support service resources

may be shared by multiple CUSTOMERS. Controls and tests will be proportionate to the risk; no claim of physical isolation will be made without a specific contract and evidence.

Dedicated environments and server management

In a dedicated environment, the PROVIDER manages the resources expressly reserved for the CUSTOMER, within the contracted layer. This may cover provisioning, secure configuration, updates, monitoring, capacity, administrative accounts, technical logging, backup, recovery and incident response. Excluded or jointly managed items must be stated in the Service Order.

The PROVIDER's responsibility for administering the environment does not turn third-party physical infrastructure, cloud services, connectivity or licensed software into its own resources. The PROVIDER is responsible for the selection, configuration and management it undertakes; the external provider is responsible for its layer; and the CUSTOMER is responsible for users, data, terminals and decisions under its control.

Backup and recovery

Frequency, retention, scope, encryption, location, restoration tests, RPO and RTO only constitute a commitment when recorded in the accepted plan or Order. Backup is a recovery control and does not replace a historical archive. The free 7-day evaluation does not include a backup or recovery guarantee, unless an obligation has been expressly accepted before activation; proportionate security measures and legal duties remain enforceable.

In the free trial, the CUSTOMER must perform or request the necessary exports before the trial ends. Without a contract or legally necessary preservation, operational content will be deleted or anonymized within 30 calendar days after the end of the trial; any residual backup copies will be purged within 90 days after the end of the trial, with restricted access and no operational reuse. The periods will be validated against the architecture before signature. Statutory retention and the lawful exercise of rights follow their own periods and purposes. The trial does not guarantee retention of recordings for 90 days or recovery of content already deleted.

Document control

Field	Record
Entity responsible for the document	COREPTT TECNOLOGIA LTDA
Coordination and legal review	Responsible person to be appointed by the PROVIDER before signature
Sales and contracting	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com
Revision and date	1.3 • 14 October 2026
Status	Draft for legal review



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Enterprise Agreement

General terms for licenses services equipment and connectivity

corePTT platform

Compliance and governance
Security and data protection

07

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 Enterprise Agreement

General terms for licenses services equipment and connectivity

Responsible provider	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Sales and contracting	sales@coreptt.com
Registered telephone number	(11) 9839-0601
Legal privacy and integrity	legal@coreptt.com
Brand and platform	corePTT
Revision	1.3
Revision date	October 14, 2026

This agreement governs the business relationship between the PROVIDER and the CUSTOMER. The Order Form defines what has been purchased; this instrument governs performance, payment, responsibilities, intellectual property, data, security, term and termination.

Provider identification

The PROVIDER is 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.

Sales and contracting: sales@coreptt.com. Registered telephone number: (11) 9839-0601. Legal, privacy, integrity and security: legal@coreptt.com.

The PROVIDER is the legal entity responsible for the commitments it undertakes in corePTT instruments. The CUSTOMER and the representatives of both parties shall be identified in the applicable instrument and must have authority to approve the scope and sign.

1 Parties and contractual documents

This Enterprise Agreement is entered into by 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, referred to as the PROVIDER, and the legal entity identified in the Order Form, referred to as the CUSTOMER. The PROVIDER and the CUSTOMER are the Parties, represented by persons authorized to enter into the agreement.

The contractual documents comprise the Order Form, this Agreement, the Technical Annex, the DPA, the SLA, the Acceptable Use Policy and any other terms expressly received and accepted, identified by title, version and date. In the event of a conflict, the Order Form prevails regarding scope and price; the DPA regarding processing on behalf of the CUSTOMER; the SLA regarding service levels; and this Agreement

regarding all other matters, subject to mandatory legal provisions. Future policies shall not be incorporated automatically, and there shall be no unilateral retroactive amendment; contractual amendments require a written agreement accepted by the Parties.

2 Subject matter

The PROVIDER shall supply the modules, licenses, professional services, support, equipment and connectivity items selected in the Order Form. Any item not selected is excluded from the subject matter, even if it appears in a presentation, demonstration, previous proposal or public material.

3 Nature of the PROVIDER activities

The PROVIDER makes the corePTT platform available and maintains it, and provides the implementation, integration, administration and support services defined in the Order Form. Third-party equipment, operating systems, networks, cloud services and components remain subject to the rights of their owners. Integration or commercialization does not make the PROVIDER a manufacturer of third-party equipment or an authorized telecommunications service provider; where connectivity is provided, the responsible party shall be identified.

4 Order Form

Each Order Form must be completed and accepted by authorized representatives before commercial activation, specifying quantities, modules, users, features, limits, environment, equipment, services, schedule, acceptance criteria, price, currency, taxes, payment, term, support, SLA, retention, hosting, service providers and responsibilities. A blank field or an unselected item does not imply that it has been contracted; material outstanding issues prevent activation of the corresponding scope. Separate Order Forms are independent unless expressly cross-referenced.

5 Implementation

Implementation may include discovery, design, configuration, integration, testing, training and go-live. The schedule begins when the PROVIDER receives the information, access credentials, equipment and approvals that depend on the CUSTOMER. Delays in these dependencies shall adjust the affected dates without placing the PROVIDER in default.

6 Acceptance criteria

The CUSTOMER shall perform the tests specified in the Technical Annex, within the period and through the responsible persons indicated in the Order Form, and report reproducible nonconformities, identifying the requirement, evidence and impact. A preference or improvement outside the scope does not prevent acceptance of a requirement that has been met. Acceptance shall be documented by authorized responsible persons; silence, use during a free evaluation or simple access to the platform does not convert the trial into a paid engagement or replace express commercial acceptance.

7 License

The license is temporary and limited to the CUSTOMER, authorized users, contracted quantities and contracted term. It does not permit sublicensing, unauthorized resale, reverse engineering, removal of proprietary notices, copying beyond what is necessary or access to source code, except where the law does not permit such restrictions.

8 Third parties and open source

Third-party and open-source components may form part of the solution. Their applicable licenses shall be respected and, where required, made available to the CUSTOMER. The PROVIDER shall not contractually reduce any right granted directly by an open-source license.

9 PROVIDER obligations

- provide the service with professional diligence and in accordance with the contractual documents;
- maintain personnel or partners appropriate to the scope undertaken;
- protect confidential information and personal data under its responsibility;
- report material impediments, applicable incidents and relevant known dependencies;
- provide the support and reports specified in the selected plan;
- comply with the laws applicable to its own activities.

10 CUSTOMER obligations

- designate persons responsible for commercial, technical, administrative, security and privacy matters;
- provide accurate requirements, access credentials, infrastructure, connectivity and decisions within the project deadlines;
- administer users, permissions, devices and lawful use of the environment;
- inform workers and other data subjects about recording, location tracking and monitoring;
- maintain alternative means for operations whose risk does not permit interruptions;
- pay the amounts and taxes for which it is responsible;
- not require the PROVIDER to perform processing or configuration contrary to law.

11 Authorized administrators

The PROVIDER may carry out instructions from registered administrators and contacts, subject to the authority granted, validation appropriate to the risk, and indications of fraud or actions beyond their authority. The CUSTOMER shall update the list without delay. Revocations and suspicions received shall be addressed promptly according to their criticality; each Party's responsibility for earlier or subsequent acts shall be determined according to its conduct, control and applicable law.

12 Equipment

Sale, rental and loan for use shall be identified by item, serial number and delivery condition. The CUSTOMER shall inspect the goods, preserve labels and use appropriate accessories. Manufacturer warranties, wear and tear, accidental damage, loss, theft, batteries, misuse and returns shall be governed by the Order Form and the equipment-specific policy.

13 Connectivity

Where SIM cards or plans are included, the Order Form shall identify the carrier, data allowance, speed, coverage, roaming, use policy and party responsible for regulatory matters. The PROVIDER does not guarantee a signal in every location or control public network unavailability. The CUSTOMER must validate coverage in the operating areas before acceptance.

14 Critical use

The CUSTOMER shall maintain alternative communications and contingency arrangements for emergencies, protection of life, hazardous processes and essential continuity. A production project involving critical use requires specific risk analysis, redundancy, testing, responsibilities, SLA and

acceptance. The free evaluation must not be used as the sole means of critical operation; the platform does not replace public emergency services.

15 Support and SLA

Hours, priorities, channels, availability and credits are those defined in the SLA and the Order Form. The first-response time is not a resolution time. The PROVIDER may reclassify a support ticket with justification based on the demonstrated impact.

16 Scope changes

A change in requirements, quantities, integration, location, schedule or assumptions shall be assessed for its impact on price, time, risk and data protection. Performance depends on written approval by the Parties. Emergency assistance does not permanently change the scope without subsequent formalization.

17 Price and invoicing

Amounts, currency, frequency, due dates and payment methods are set out in the Order Form. Recurring licenses may be invoiced in advance; variable services, overages and authorized expenses may be invoiced after their amounts have been determined. A substantiated dispute must be raised within the period specified in the Order Form and does not suspend payment of the undisputed portion.

18 Taxes

Each Party shall bear the taxes imposed on it by law. Mandatory withholdings must be documented. If a legislative change creates a charge directly applicable to the service, the Parties shall negotiate an economic adjustment to the extent permitted by the agreement and the law.

19 Price adjustment

Recurring prices shall be adjusted at the intervals and according to the index specified in the Order Form. If no index is specified, the IPCA shall apply after the minimum permitted period. A supplier price increase, exchange-rate change or scope change does not automatically adjust prices outside the agreed rule, but may support a proposed revision upon renewal or for the affected component.

20 Payment default

Late payment subjects the CUSTOMER to the charges specified in the Order Form and permits suspension following notice and a cure period, except where there is a risk of fraud or repeated default. Before suspension, the PROVIDER shall consider the operational impact and, where feasible, limit the measure to the unpaid component.

21 Intellectual property

Each Party retains ownership of what it owned before the agreement. Configurations, documentation and deliverables specifically created shall be licensed or assigned as provided in the Order Form. The PROVIDER retains ownership of its tools, methods, libraries, reusable components and general knowledge, without incorporating the CUSTOMER's confidential information.

22 CUSTOMER data

The CUSTOMER and the respective data subjects retain their rights over their data and content. The PROVIDER shall carry out the processing necessary for the service under lawful instructions, and shall not sell the environment's personal data or use communications content for advertising or training AI models

without a specific agreement and an appropriate legal basis. Aggregated metrics require effective anonymization and protection of the CUSTOMER's confidential information.

23 Data protection

The Parties shall comply with the LGPD and the DPA, with roles defined according to purpose. The CUSTOMER is the controller of user, communications and location data that it processes for its purposes, and the PROVIDER processes that data under documented instructions. The PROVIDER may be an independent controller for commercial registration, contract management, invoicing, fraud prevention, legal obligations and defense of its own rights. Security of the environment on behalf of the CUSTOMER does not automatically change the PROVIDER's processor role. Monitoring and recording require a legal basis, transparency and safeguards defined by the controller; contractual acceptance is not blanket consent from users.

24 Security

The PROVIDER shall maintain measures proportionate to the risk and disclose relevant architecture, controls and exceptions. The CUSTOMER shall protect networks, devices, identities and integrations under its control. A specific certification or technical warranty forms part of the engagement only if expressly accepted in the Technical Annex and supported by valid evidence and an applicable scope; this Agreement does not assert any nonexistent certification.

25 Incidents

A Party identifying an incident affecting data or the service shall notify the other without undue delay, providing available information and updates for containment and assessment without awaiting the definitive conclusion of the investigation. The PROVIDER, as processor, shall notify the controller; the controller shall assess mandatory notifications to the ANPD and data subjects and make them within the statutory deadlines, with the processor's cooperation. Each Party's own obligations and costs shall be determined according to cause, control and law.

26 Confidentiality

Information identified as confidential, or reasonably understood to be confidential, shall be used only to perform the agreement and disclosed only to persons who need to know it and are bound by confidentiality obligations. This obligation does not cover information that is public without a breach, was already lawfully known, was received from a third party without restrictions, or was independently developed.

If disclosure is required by law or an authority, the receiving Party shall inform the other where permitted and limit the content to what is necessary. The confidentiality obligation continues for three years after termination; trade secrets and personal data remain protected for the period required by their nature and by law.

27 Warranties

The PROVIDER warrants that it shall provide the services with professional diligence and correct reproducible nonconformities under its control in accordance with the support terms. It does not warrant that the service shall be uninterrupted, free from all errors or compatible with unapproved components. Statutory warranties that cannot be excluded remain in effect.

28 Limitation of liability

Except in cases of willful misconduct, gross negligence, fraud, breach of confidentiality, intellectual property infringement, breach of a data protection obligation attributable to the Party, or circumstances in which the

law does not permit a limitation, each Party's liability for direct damages arising from the commercial operation is limited to the amount paid or payable by the CUSTOMER in the twelve months preceding the event. The application and extent of this limit depend on its legal validity in the specific case and do not exclude warranties, compensation or nonwaivable rights. The limit does not apply to the free evaluation, whose free nature does not release the Parties from statutory duties.

Neither Party is liable for indirect damages, remote lost profits or avoidable losses where there is no causal link. This exclusion does not prevent reimbursement of direct and reasonable costs of incident response, restoration, notification or a judgment in favor of a third party where legally attributable.

29 Third-party indemnification

A Party that causes a third-party claim by breaching its obligations shall defend and indemnify the other in proportion to its responsibility, provided that it receives notice, cooperation and reasonable control of the defense. A settlement that imposes an obligation or an admission on the protected Party requires that Party's consent.

30 Compliance and anti-corruption

The Parties shall comply with applicable law, including anti-corruption rules and Law nº 12.846/2013 where applicable, applicable economic sanctions, export rules and their own labor obligations. Improper benefits, fraud, unlawful favoritism and use of the relationship to circumvent purchasing processes, authorization levels or internal controls are prohibited. Approvals and changes shall be recorded by authorized representatives. Suspicions of fraud, conflicts of interest or irregularities may be reported to legal@coreptt.com, with restricted access to the investigation and no retaliation for good-faith reports.

31 Audit

The CUSTOMER may request reasonable evidence of compliance once a year or after a significant incident. An on-site audit requires justification, confidentiality, prior notice and preservation of other customers' security. Extraordinary costs shall be borne by the requesting party, unless a material nonconformity by the PROVIDER is confirmed.

32 Subcontracting

The PROVIDER may engage suppliers to perform part of the service while remaining responsible for its undertaken obligations. Subprocessors with access to data are governed by the DPA. The CUSTOMER may not transfer operation of the platform to a third party outside its group without authorization.

33 Term and renewal

The commercial term begins on the date entered and accepted in the Order Form, after the engagement has been formalized. The initial term, minimum commitments, renewal and notice of nonrenewal shall be expressly selected and accepted. Automatic renewal of a commercial service shall exist only if selected and accompanied by the term, conditions and notice in the Order Form; a blank field does not authorize it. Obligations concerning payment of valid amounts, confidentiality, intellectual property, data and liability survive for the applicable period. The free evaluation does not begin a paid term, renew automatically or convert into a commercial engagement.

34 Termination

The Party that has fulfilled its obligations may terminate for a material breach not cured within thirty days of notice, unless the Order Form specifies a different period or immediate action is necessary. Termination is

also permitted for insolvency, serious unlawful use or definitive impossibility of the subject matter. Overdue amounts and minimum commitments remain enforceable according to the cause.

35 Exit and return of data

Upon termination of the service, the PROVIDER shall make the export specified in the Order Form available for the contracted period. Migration, format transformation and additional assistance shall be charged where they are outside the scope. After that period, data shall be deleted or anonymized under the DPA, subject to backups, legal obligations and preservation of evidence.

36 Force majeure

Neither Party is liable for delays caused by an unavoidable event outside its reasonable control, provided that it gives notice, mitigates the impact and resumes performance when possible. Lack of financial resources does not constitute force majeure. If the impossibility continues for more than sixty days, either Party may terminate the affected item without a penalty for the future period.

37 Communications

Contractual notices shall be sent to the contacts in the Order Form, with records of dispatch and receipt according to the agreed medium. Sales and contracting: sales@coreptt.com; registered telephone number: (11) 9839-0601. Legal, privacy, integrity and security: legal@coreptt.com. Changes of address and contact details shall be reported. Operational tickets shall be directed to the support channels defined in the Order Form; they do not replace a formal notice of termination or dispute without confirmation of receipt by the responsible person, and urgent security alerts must be escalated promptly.

38 Assignment

Neither Party shall assign the agreement without the other's consent, which shall not be withheld without reasonable grounds. Assignment is permitted in a corporate reorganization or substantial sale of the operation, provided that the successor assumes the obligations and the assignment does not reduce data protection or the ability to perform.

39 Electronic signature

The Parties may sign physically or electronically through a method accepted by both that records authorship, integrity, version, date and time. The signatory shall declare their authority to represent the relevant Party. Article 10 of Provisional Measure nº 2.200-2/2001 and the requirements of the method used apply. Copies and counterparts signed at different times form a single instrument provided that they correspond to the same accepted version.

40 Governing law and jurisdiction

Brazilian law applies. The Parties shall seek an agreed solution through representatives with decision-making authority, without preventing urgent measures or the exercise of rights. The courts of the Judicial District of Campinas/SP are chosen because of their connection to the PROVIDER's registered office, subject to mandatory statutory jurisdiction and consumer protection rules where applicable.

Development and intellectual property

The PROVIDER or its licensors retain the rights to corePTT, the platform, preexisting components, reusable connectors, methods, documentation and internal tools. Developments exclusively for the

CUSTOMER shall be assigned only when the Order Form expressly defines the subject matter, code, documentation, remuneration and extent of the assignment.

Contracting configuration, integration or customization does not imply transfer of source code or exclusivity. Open-source and third-party components remain subject to their own licenses. The CUSTOMER's data and content do not become the PROVIDER's property.

Development customization and acceptance cycle

On-demand services shall be described by scope, assumptions, dependencies, deliverables, stages, schedule, estimate, price and objective acceptance criteria. A change in requirements, integration, volume, manufacturer, version, infrastructure or data may trigger an impact assessment and an additional proposal. The CUSTOMER shall provide access credentials, information, decisions and persons responsible for validation within the agreed periods.

A defect is a reproducible discrepancy between the delivery and the approved criterion. Enhancements, new rules, subsequent third-party adaptations and changes of preference are not defect corrections and may be treated as new requests. Support, enhancement maintenance, warranty and incorporation into the standard version depend on the Order Form.

Hosting retention and backups

The CUSTOMER may contract a shared or dedicated environment. The PROVIDER shall be responsible for managing the servers and components included in the managed service, subject to the responsibility matrix. Exclusivity of a physical machine, region, provider, IP address, database, network or team shall exist only where expressly stated.

In the commercial operation, retention categories and periods shall be selected and accepted in the Order Form and the DPA. A rolling window of up to 90 days for recordings or other content applies only when expressly contracted and compatible with the controller's purpose; it is not a general storage period for all data. Longer retention, archiving, immutability, recurring export and special preservation depend on a valid additional scope. Frequency, backup retention, RPO, RTO and restoration are separate fields and must not be confused with content retrieval.

Free 7 day evaluation

The free evaluation, where authorized in a separate instrument, lasts 7 calendar days, equivalent to 168 hours from activation as communicated to the CUSTOMER. Before access is released, the activation schedule must record the start, end, Brasília time zone, responsible persons, limits, features, hosting and service providers. The license costs R\$ 0,00; additional services, connectivity and equipment depend on their own previously accepted terms. At the end, access may be suspended without automatic renewal, automatic conversion to a paid plan, retroactive charges for the trial or any obligation to purchase. A free extension requires written approval and a new end date. Continuation depends on an accepted proposal and formal contracting through sales@coreptt.com; merely contacting sales does not extend access or guarantee preservation of data.

During the free trial, the CUSTOMER must perform or request the necessary exports before the trial ends. Without an engagement or legally necessary preservation, operational content shall be deleted or anonymized within 30 calendar days after the end; any residual backup copies shall be purged within 90 days after the end, with restricted access and no operational reuse. The periods shall be validated against the architecture before signature. Legal retention and the regular exercise of rights follow their own periods and purposes. The trial does not guarantee retention of recordings for 90 days or recovery of content already deleted.

External dependencies and allocation of responsibility

The PROVIDER is not liable for unavailability caused exclusively by a third-party network, service, API, equipment or software outside its reasonable control, provided that it did not contribute to the event and fulfills the diagnosis, communication, mitigation and escalation obligations specified in the SLA. No provision excludes liability that cannot be excluded under applicable law.

Document control

Field	Record
Document owner	COREPTT TECNOLOGIA LTDA
Coordination and legal review	Responsible person to be designated by the PROVIDER before signature
Sales and contracting	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com
Revision and date	1.3 • October 14, 2026
Status	Draft for legal review

PROVIDER	CUSTOMER
COREPTT TECNOLOGIA LTDA	Registered company name specified in the Order Form
CNPJ 69.599.966/0001-93	CNPJ specified in the Order Form
Representative name and position	Representative name and position
Electronic signature	Electronic signature



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Data Processing Agreement

Agreement between controller and processor under the LGPD

corePTT platform

Compliance and governance
Security and data protection

08

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 Data Processing Agreement

Agreement between controller and processor under the LGPD

Responsible provider	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Sales and contracting	sales@coreptt.com
Registered telephone number	(11) 9839-0601
Legal privacy and integrity	legal@coreptt.com
Brand and platform	corePTT
Revision	1.3
Revision date	October 14, 2026

This DPA defines roles, instructions, security measures, subprocessors, incidents, rights, audits, retention and international transfers for data processed in the CUSTOMER's environment.

Provider identification

The PROVIDER is COREPTT TECNOLOGIA LTDA, trade name 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.

Sales and contracting: sales@coreptt.com. Registered telephone number: (11) 9839-0601. Legal, privacy, integrity and security: legal@coreptt.com.

The PROVIDER is the legal entity responsible for the commitments it undertakes in the corePTT instruments. The CUSTOMER and the representatives of both parties will be identified in the applicable instrument, with authority to approve the scope and sign.

1 Purpose of the DPA

This DPA governs data processing carried out by the PROVIDER on behalf of the CUSTOMER in corePTT and clarifies each controller's own purposes. It forms part of the commercial engagement or the free 7-day evaluation only when identified by title, version and date and made available before acceptance. Data protections do not make commercial terms or the production SLA applicable to the trial. The relevant annexes and instructions must be completed and validated before activation.

2 Definitions

The definitions in Law No. 13.709 of 2018 apply. For this DPA, CUSTOMER Data means personal data entered, transmitted, generated or stored in the environment under the CUSTOMER's instructions;

Subprocessor means a third party engaged by the PROVIDER to process such data; Incident means a confirmed event that compromises confidentiality, integrity, availability or authenticity.

3 Roles of the Parties

The CUSTOMER is the controller of user, communications and location data processed for its purposes and determines the essential elements of this operation. The PROVIDER acts as processor under lawful and documented instructions. It may be an independent controller for business registration, negotiation, contract management, billing, fraud prevention, compliance with its own obligations and exercise of rights. The role in security and logs depends on the specific purpose: measures performed on behalf of the CUSTOMER do not automatically make the PROVIDER an independent controller.

If a Party determines a purpose incompatible with its declared role, it will be responsible as the corresponding processing agent for that operation, without automatically transferring the consequences of its decision to the other Party.

4 Description of processing

Element	Description
Subject matter	platform operation, support, hosting, transmission, recording, location, integrations and termination in accordance with the Order
Duration	service term and the applicable exit, retention, backup or statutory obligation period
Data subjects	users, administrators, workers, service providers, representatives and people communicated with in the CUSTOMER's environment
Data	registration, authentication, device, network, PTT events, location, content, logs, support and other categories selected in Annex A
Operations	collection, receipt, access, organization, storage, transmission, retrieval, support, export, blocking and erasure
Purpose	deliver, protect, maintain and terminate the contracted features in accordance with the CUSTOMER's instructions

5 Documented instructions

The applicable instrument, the Order or activation form, the annexes to this DPA and the instructions of authorized administrators constitute the documented instructions, within the agreed authority and purposes. Support tickets and configuration changes do not authorize a material change in purpose, subprocessors, transfer or retention without the corresponding approval process. The PROVIDER will notify the CUSTOMER of any instruction it considers unlawful and may suspend it pending clarification. The CUSTOMER remains responsible for determining its legal basis and ensuring transparency.

6 CUSTOMER obligations

- ensure a legal basis, a legitimate purpose, transparency and respect for data subjects' rights;
- assess the necessity and proportionality of recording, location tracking and worker monitoring;
- configure access, retention and features in accordance with its policy;
- not enter sensitive, biometric or children's data without a specific assessment and instruction;
- keep the information in the Annexes accurate and communicate changes;

- make the notifications to the ANPD and data subjects that fall to the controller.

7 PROVIDER obligations

- process CUSTOMER Data only to carry out the instructions and applicable legal obligations;
- restrict access to authorized persons bound by confidentiality;
- implement and maintain the measures in Annex B, in accordance with the contracted environment;
- assist the CUSTOMER with available information on rights, incidents, impact assessments and the authority;
- maintain sufficient records to demonstrate compliance with its obligations as processor;
- erase or return data at the end of the service in accordance with this DPA.

8 Confidentiality and authorized persons

The PROVIDER will ensure that persons with access receive appropriate guidance, use the data only in their authorized role and are bound by a duty of confidentiality during and after their engagement. Exceptional support access must be restricted, logged where technically possible and revoked when the need ends.

9 Security measures

The minimum measures are set out in Annex B and will be applied in accordance with the nature, volume, context, purpose and risk. The CUSTOMER acknowledges that controls dependent on its environment, such as user, device, local network and federated identity management, are its responsibility. A material change that reduces protection requires notice and contractual handling.

10 Subprocessors

The CUSTOMER authorizes the subprocessors identified by name in a list delivered before activation, with the relevant service, role, country, region and contact details. A list on an external page must be incorporated by version and date, with a copy or record retained; future changes are not automatically incorporated. The PROVIDER will impose compatible duties concerning security, confidentiality, instructions, incidents and erasure and will remain responsible for the obligations it assumes and for supervising the subprocessors it selects.

The addition or replacement of a subprocessor will be communicated before the affected processing, with information and an assessment period defined in the annex. The CUSTOMER may submit a reasoned objection based on data protection. Material changes will be formalized through the contractually accepted procedure; the Parties will seek a secure alternative. If no viable alternative is available, the component may be terminated without a penalty for the future period, preserving return, erasure, legal obligations and non-waivable rights.

11 International transfer

An international transfer will take place only when the country, exporter, importer, purpose, categories, onward transfers, duration and measures are described in Annex C, with a valid legal ground and mechanism. This definition must be known and validated before activation. A material change in destination or mechanism requires prior information and formalization. The PROVIDER will supply the available elements for the assessment, in compliance with the LGPD and applicable regulations.

If the selected mechanism is the standard contractual clauses under CD ANPD Resolution No. 19 of 2024, Sections I, II and III of the official text will be annexed in full and without modification to the instrument between the exporter and importer. No commercial provision may conflict with them.

12 Data subject requests

If the PROVIDER receives a request relating to CUSTOMER Data, it will verify identity proportionately, provide the CUSTOMER's contact channel or forward the request without responding on its merits, unless instructed or legally required to do so. The PROVIDER will make reasonable functions and information available to enable the CUSTOMER to fulfill the request within the applicable periods.

13 Incident involving CUSTOMER Data

The PROVIDER will notify the CUSTOMER, as controller, of an identified incident involving its data without undue delay, with available information and updates for assessment and containment. It will aim to provide the initial notification within 24 hours of becoming aware, without this target authorizing unjustified delay or waiting for the investigation to conclude. The annex may define a shorter operational period. The initial notification may be incomplete and does not constitute an admission of fault.

The PROVIDER will report, as available: nature and date; categories of data and data subjects; affected environments; measures before and after the incident; likely impacts; containment and mitigation actions; subprocessor identification; and the responsible contact. The PROVIDER will preserve evidence and maintain a record for the statutory period.

14 Notification to the ANPD and data subjects

The CUSTOMER, as controller, will assess the existence of significant risk or harm and make mandatory notifications to the ANPD and data subjects within the statutory periods. Under CD ANPD Resolution No. 15 of 2024, where applicable, notification is made within three business days of becoming aware that the incident affected personal data, subject to the relevant legal, sector-specific and differentiated rules. The PROVIDER will cooperate with available information and updates and will notify on behalf of the CUSTOMER only with formal authorization or under an obligation of its own. No contractual rule extends a statutory deadline.

15 Impact assessment report and consultation

The PROVIDER will supply available information and necessary cooperation regarding architecture, measures, subprocessors and operations to support the CUSTOMER's impact assessments. Additional work outside the obligations already assumed will depend on a previously accepted scope and price; statutory cooperation duties will not be conditional on purchasing an additional service. The decision on whether a report is needed, its content and its submission remains with the controller.

16 Audit and demonstration

The PROVIDER will answer a reasonable questionnaire and make existing evidence available. An audit must take place no more than once a year, except in the event of an incident or an authority's requirement, with notice, a defined scope, an independent auditor, confidentiality and protection of other customers. The CUSTOMER bears extraordinary costs unless the audit confirms a material breach by the PROVIDER.

17 Authority requests

The PROVIDER will assess validity and limit the response to what is necessary. Where permitted, it will notify the CUSTOMER before disclosing CUSTOMER Data. International requests will be handled in accordance with the applicable legislation, transfer mechanism and commitments.

18 Return and erasure

For the commercial service, export, the exit period, formats and assistance will be set out in the Order. After this period, the PROVIDER will erase or anonymize active data and purge backups according to the completed and accepted cycles and maximum periods, without operational use. Statutory retention, blocking, a valid authority order and the lawful exercise of rights will be restricted to the necessary purpose and period. In the free trial, the specific erasure and backup limits described in the 7-day agreement and this DPA apply; subsequent access is not guaranteed.

19 Anonymized data and metrics

The PROVIDER may produce aggregated technical metrics for capacity, quality and security, provided that it applies a reasonable anonymization process and does not attempt to reidentify data subjects or disclose the CUSTOMER's confidential information. Data that is merely pseudonymized remains subject to this DPA where it can be associated with a person using additional information.

20 Liability

Each Party is responsible for its acts and omissions under the LGPD, this DPA and the Agreement. A Party that acts outside the instructions or determines its own purpose is responsible in the corresponding role. The contractual allocation does not limit data subjects' rights or the ANPD's powers.

21 Precedence and term

This DPA remains in force while the PROVIDER processes the CUSTOMER's data and takes precedence in data protection matters, preserving mandatory rules and without changing the price or technical scope. The accepted title, version and date must be recorded in the principal instrument. Future policies and retroactive changes are not automatically incorporated; material changes require a written amendment through the accepted process. Confidentiality, erasure, cooperation, pending audits and liability survive for the necessary period.

22 Annex A processing details

Field	Contractual selection or description
Active modules	voice ☐ video ☐ messages ☐ files ☐ GPS ☐ recording ☐ console ☐ API ☐
Data subjects	employees ☐ service providers ☐ visitors ☐ third parties communicated with ☐ others _____
Registration data	name ☐ email ☐ telephone ☐ company ☐ position ☐ identifier ☐
Technical data	IP ☐ device ☐ system ☐ telecommunications carrier ☐ logs ☐ SIM identifiers ☐
Content	audio ☐ video ☐ text ☐ files ☐ recordings ☐
Location	current ☐ history ☐ accuracy ☐ geofence ☐
Anticipated sensitive data	no ☐ yes ☐ categories, purpose and basis: _____
Children and adolescents	not anticipated ☐ anticipated ☐ safeguards: _____

Field	Contractual selection or description
Retention	in accordance with the Service Order and the environment's retention schedule
Legal basis and information for data subjects	[complete by purpose and category before activation]
Environment and purpose	commercial [] free 7-day evaluation []; instrument reference: [complete]
Controller representative and contact	[name, position and email to be completed]
Processor representative and contact	[name and position to be completed]; legal@coreptt.com
Commercial exit period	[complete the period, access, format and responsible person or indicate not contracted]
Active data erasure in the trial	within 30 days after the end, subject to legal exceptions; validate the architecture before signing
Residual copies in the trial	purge within 90 days after the end, without operational reuse; validate the architecture
Commercial backup	[frequency, categories, access, retention and maximum purge period to be completed]

23 Annex B minimum measures

Domain	Measures
Governance	responsible persons, inventory, risk assessment, policies, exceptions and periodic review
Access	individual accounts, least privilege, review, deactivation and administrative MFA where supported
Confidentiality	confidentiality commitments, guidance and restriction based on functional need
Technical protection	secure protocols in accordance with the architecture, secrets management, segmentation and endpoint protection
Development and change	version control, review, testing, dependencies, approval and rollback
Vulnerabilities	monitoring, classification, remediation according to risk and compensating controls
Logs	logging of relevant actions, protection against alteration and proportionate retention
Continuity	backup, restoration, capacity and recovery plan in accordance with the Technical Annex
Incidents	alert channel, classification, containment, evidence, notification and records retained for five years

Suppliers	assessment by criticality, contract, subprocessor list and valid transfer
Erasure	return, deletion from the active environment, backup overwriting and secure disposal

24 Annex C international transfers

Field	Information to be completed where applicable
Exporter	legal name, country, role and contact
Importer	legal name, country, role and contact
Countries and regions	_____
Purpose and duration	_____
Categories and data subjects	_____
Onward transfers	_____
Mechanism under Article 33	adequacy ☐ standard contractual clauses ☐ specific ☐ other ground _____
Additional measures	_____
Reference to the annexed mechanism	[document, version, date and signatures where applicable]
Validation before activation	[responsible persons from the CUSTOMER and the PROVIDER, date and acceptance record]

Where standard contractual clauses are selected, the official Annex to CD ANPD Resolution No. 19 of 2024, completed and without modification to its mandatory sections, must be attached to this DPA.

Integrations and subprocessors

The PROVIDER may engage providers of infrastructure, communications, monitoring, support or other subprocessors necessary to perform the service. Each engagement must impose compatible duties of confidentiality, security, processing in accordance with instructions and cooperation in handling data subject requests and incidents.

The DPA does not automatically transfer to the PROVIDER responsibility for independent controllers' own decisions, nor does it permit the PROVIDER to exempt itself from obligations relating to the subprocessors it selects to process CUSTOMER Data.

Retention and lifecycle instructions

The categories and retention periods for commercial operations must be completed and accepted in the Order and Annex A. A rolling window of up to 90 days for recordings or other content requires express selection and does not automatically apply to all data or to the free trial. The CUSTOMER must confirm compatibility with the legal basis, necessity, transparency, retention schedule and data subjects' rights.

Longer retention must be specified in a valid instruction and a specific engagement. The PROVIDER may refuse an instruction that is manifestly unlawful, excessive, insecure or technically unfeasible, stating the

grounds and proposing an alternative. Termination, return, erasure, blocking and legal preservation will be recorded according to the nature of the environment.

Evaluation environments

In the free 7-day evaluation, equivalent to 168 hours from the notified activation, fictitious or anonymized data will be preferred where sufficient. Real content, voice, video, messages and location will be processed only through authorized features and with a legal basis and transparency provided by the controller. Sensitive data and children's or adolescents' data are excluded from the evaluation unless specifically agreed in advance and the legal requirements are met. In the free trial, the CUSTOMER must perform or request the necessary exports before the end. Without an engagement or legally necessary preservation, operational content will be erased or anonymized within 30 calendar days after the end; any residual backup copies will be purged within 90 days after the end, with restricted access and without operational reuse. The periods will be validated against the architecture before signing. Statutory retention and the lawful exercise of rights follow their own periods and purposes. The trial does not ensure retention of recordings for 90 days or recovery of content already erased.

Backup restoration and secure erasure

Backups processed by the PROVIDER follow the instructions, access controls and cycles defined in the plan. Erasure requests cover active data and, within technical limits, recoverable copies. Where a granular backup change would compromise its integrity, the information will remain blocked and will be erased by expiry or secure overwriting, subject to any legal obligation.

Shared and dedicated infrastructure

The shared or dedicated nature of the infrastructure does not change the processing roles. The PROVIDER must maintain segregation, restricted access and measures proportionate to the risk. Features and subprocessors, including the hosting region, will be identified to the extent necessary for transparency, security and international transfer rules.

Document control

Field	Record
Document owner	COREPTT TECNOLOGIA LTDA
Coordination and legal review	Responsible person to be appointed by the PROVIDER before signing
Sales and contracting	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com
Revision and date	1.3 • October 14, 2026
Status	Draft for legal review

25 Signatures

PROVIDER	CUSTOMER
COREPTT TECNOLOGIA LTDA	Legal name stated in the Service Order
CNPJ 69.599.966/0001-93	CNPJ stated in the Service Order
Representative's name and position	Representative's name and position
Electronic signature	Electronic signature



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Support and Availability SLA

Measurement, priorities, support, maintenance and credits

corePTT platform

Compliance and governance

Security and data protection

09

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 Support and Availability SLA

Measurement, priorities, support, maintenance and credits

Responsible provider	COREPTT TECNOLOGIA LTDA
Trading name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Sales and contracting	sales@coreptt.com
Registered telephone	(11) 9839-0601
Legal matters privacy and integrity	legal@coreptt.com
Brand and platform	corePTT
Revision	1.3
Revision date	14 October 2026

This SLA defines measurement and support for paid corePTT commercial services. Targets apply only to the components and plan completed and accepted in the Order before activation; the 7-day free evaluation follows its own agreement and is not included in commercial targets or credits.

Provider identification

The PROVIDER is COREPTT TECNOLOGIA LTDA, trading name COREPTT TECNOLOGIA, registered with the CNPJ under 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.

Sales and contracting: sales@coreptt.com. Registered telephone: (11) 9839-0601. Legal matters, privacy, integrity and security: legal@coreptt.com.

The PROVIDER is the legal entity responsible for the commitments it undertakes in the corePTT instruments. The CUSTOMER and the representatives of both parties will be identified in the applicable instrument, with authority to approve the scope and sign.

1 Purpose

This SLA defines availability and support for components hosted and administered by the PROVIDER that are selected in the Order. Professional services, equipment, third-party applications, carriers and the CUSTOMER environment are included in the SLA only when an express target is specified.

2 Plans

Plan	Standard coverage	Indicative monthly target
Essential	business days from 8h to 18h Brasília time	99.5 percent
Operational	P1 on a 24 by 7 basis and other priorities on business days	99.9 percent
Customized	as specified in the Service Order	as specified in the Service Order

The plan, components, targets, measurement points and intervals, hours, channels and contacts must be selected and accepted before commercial activation. An indicative percentage without selection does not constitute an automatic commitment. If no availability SLA is contracted, this will be expressly indicated in the Order, without excluding duties of diligence, security and compliance with the law.

3 Available service

A component is considered available when authorized users can perform its primary function from the defined measurement points. Partial degradation may be treated as proportional unavailability when it prevents a material part of the contracted function.

4 Calculation

Monthly availability (%) = ((eligible time minus countable unavailability) / eligible time) × 100. The calculation will be performed by component and environment, for the period and time zone defined in the Order, based on the agreed measurement points and records. Exclusions must be specified, demonstrable and quantified. If eligible time is zero, the report will indicate the absence of a measurable period and will not assign a fictitious percentage. Partial degradation will follow the approved criterion for the contracted function.

5 Exclusions

- scheduled maintenance within the contracted limit;
- demonstrable action or omission by the CUSTOMER, user, integration or third party under its management, to the extent that it caused the event;
- proven failure of a device, local network, internet, carrier or supplier outside the managed scope, if the PROVIDER did not contribute and fulfills its diagnosis, communication and escalation duties;
- legitimate suspension for security, misuse, an authority order or payment default;
- force majeure and a large-scale attack that could not have been prevented by a reasonable measure;
- a beta feature, demonstration, proof of concept or version without a production commitment;
- an event without sufficient evidence after a joint investigation; the absence of an alert in the PROVIDER monitoring does not, by itself, invalidate reliable evidence presented by the CUSTOMER.

6 Maintenance

Windows and the monthly limit for excluded maintenance will be completed in the Order; without a contracted limit, maintenance time will not be automatically excluded. Scheduled maintenance will be communicated at least 48 hours in advance, unless another period is expressly accepted. Emergency maintenance may occur without advance notice to contain a risk, with the cause, impact and completion communicated as soon as possible; its exclusion from the calculation will depend on expressly agreed criteria.

7 Priorities

Priority	Criterion	Example
P1 critical	primary service unavailable for a significant operation, without a reasonable alternative	production environment inaccessible to most users
P2 high	important function degraded or unavailable, with a limited alternative	significant group or console affected
P3 medium	limited impact, without material interruption of operations	isolated failure or reduced performance
P4 low	question, request, adjustment or improvement	configuration, guidance or future request

8 Support targets

Priority	First response	Update	Workaround target
P1	30 minutes under the Operational plan	every 2 hours	4 hours when technically feasible
P2	2 business hours	daily on a business day	1 business day when technically feasible
P3	8 business hours	according to progress	planning within 3 business days
P4	2 business days	when a decision is made	according to queue and scope

Targets begin upon receipt of the ticket through the contracted channel and of the minimum information essential for diagnosis. Missing nonessential information will not unjustifiably delay the clock. The time limits are for first response, updates and workarounds, according to the selected table, and are not an unrestricted guarantee of resolution. Replacements of the table must be written and accepted in the Order.

9 Opening a ticket

The CUSTOMER must provide the environment, affected users, onset, impact, reproduction steps, evidence and an available contact. P1 tickets must be opened through the plan emergency channel, in addition to the written record. A duplicate ticket does not accelerate support and may be consolidated.

10 Classification and escalation

The initial priority may be revised after diagnosis. Any disagreement will be explained to the CUSTOMER contact. A critical incident will be escalated to the PROVIDER operations manager; security or data matters will also follow the DPA process.

11 CUSTOMER obligations

The CUSTOMER will maintain on-call contacts, grant secure access, preserve evidence and perform reasonable tests. The clock may be paused only during an essential wait for information, access, approval or testing under the CUSTOMER responsibility, with justification, recorded start and end times and notice of resumption. The pause does not change statutory privacy deadlines or mitigation obligations that can be fulfilled.

12 Monitoring and reporting

The PROVIDER will use its own monitoring or monitoring from a supplier compatible with the component. CUSTOMER measurements will be considered when reproducible. A monthly report will be provided when contracted, including availability, relevant incidents, maintenance and applicable credits.

13 Credits

Component availability	Credit on the eligible monthly fee
at or above the target	no credit
up to 0.5 percentage points below the target	5 percent
more than 0.5 and up to 2 points below	10 percent
more than 2 points below	20 percent

The SLA credit applies to the eligible recurring monthly fee of the affected component, excluding equipment, connectivity, professional services and taxes, capped at 20% in the month, unless a different rule is written in the Order. The request must be submitted within 30 days after the report is made available to the CUSTOMER, with documentation for the period. The table bands and this rule must be expressly accepted. A credit is contractual service compensation and does not exclude liability for willful misconduct, gross negligence or damage for which compensation cannot be excluded, nor does it restrict nonwaivable rights.

14 Repeated incidents

If the same component misses the target for three consecutive months, the Parties will prepare a corrective plan. If material noncompliance persists after a reasonable period, the CUSTOMER may terminate the affected component without a penalty for the future period, in addition to credits already owed.

15 Continuity and recovery

RTO, RPO, redundancy, a secondary region and disaster tests are binding only when described in the Order or Technical Annex. The availability target does not, by itself, create a guarantee of zero data loss or recovery within a specified time.

16 Security and privacy

A security event may require suspension, credential rotation or emergency maintenance. The operational classification in this SLA does not replace the assessment of risk to data subjects, DPA notification deadlines or LGPD obligations.

17 SLA revision

Changes to targets, rules, channels or scope for future periods require formalization and written acceptance, without automatic incorporation of a future version or retroactive reduction. Urgent technical security adjustments may temporarily change procedures, with records, communication and restoration of the workflow, preserving current commitments and statutory duties.

External dependencies in the availability calculation

Unavailability of an external service may be excluded from the calculation only when the component is identified as a dependency, the external cause is demonstrable and the PROVIDER did not contribute to the event. Diagnosis and escalation time will remain subject to the support targets applicable to the contracted plan.

Scope of server management

Monitoring and support cover only the layers managed by the PROVIDER and indicated in the Service Order. Shared or dedicated servers, operating systems, databases, applications, connectivity, devices, integrations and providers must have defined responsible parties. The PROVIDER will coordinate diagnosis of the layers under its management and escalation of dependencies.

Backup, restoration, RPO and RTO

The existence of a backup does not imply instant restoration or absence of loss. The maximum acceptable data loss point (RPO), recovery time target (RTO), frequency, retention, testing and restoration priority are contractual targets only when completed in the Service Order. Without these fields, best efforts compatible with the plan apply, without a specific target.

Evaluation environments

The 7-day free evaluation, equivalent to 168 hours from the communicated activation, is not included in the availability calculation or the credits under this SLA. It does not include a commercial SLA, a backup or recovery guarantee, continuous capacity or 24-hour support, unless a specific obligation is written in the agreement. Initial support will be routed through sales@coreptt.com according to scope and availability; security incidents will be reported to legal@coreptt.com and remain subject to triage, cooperation and statutory data protection deadlines.

The CUSTOMER must maintain contingency measures and must not rely exclusively on the trial for emergencies or critical processes. Formalizing service after the trial requires an accepted proposal and a formal contract; there is no automatic conversion or renewal. Data retention and purging follow the evaluation agreement and the DPA, without free retention of recordings for 90 days.

Document control

Field	Record
Document owner	COREPTT TECNOLOGIA LTDA
Coordination and legal review	Responsible person to be appointed by the PROVIDER before signature
Sales and contracting	sales@coreptt.com

Field	Record
Legal matters privacy and integrity	legal@coreptt.com
Revision and date	1.3 • 14 October 2026
Status	Draft for legal review

18 Signatures

PROVIDER	CUSTOMER
COREPTT TECNOLOGIA LTDA	Legal name indicated in the Service Order
CNPJ 69.599.966/0001-93	CNPJ indicated in the Service Order
Representative name and title	Representative name and title
Electronic signature	Electronic signature



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Service Order and Commercial Proposal

Form to define scope, pricing, data, security, SLA and acceptance

corePTT platform

Compliance and governance

Security and data protection

10

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 Service Order and Commercial Proposal

Form to define scope, pricing, data, security, SLA and acceptance

Responsible provider	COREPTT TECNOLOGIA LTDA
Trading name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Sales and contracting	sales@coreptt.com
Registered telephone	(11) 9839-0601
Legal matters privacy and integrity	legal@coreptt.com
Brand and platform	corePTT
Revision	1.3
Revision date	14 October 2026

This Order defines the corePTT commercial contract and must be completed and accepted by authorized representatives before activation. Scope, features, limits, dates, amounts, payment, support, hosting, data and responsibilities will be expressly stated. An unselected item is outside the scope; a material blank field does not authorize a presumption that it has been contracted. The 7-day free evaluation is governed by its own agreement and does not automatically convert into a paid service.

Provider identification

The PROVIDER is COREPTT TECNOLOGIA LTDA, trading name COREPTT TECNOLOGIA, registered with the CNPJ under 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.

Sales and contracting: sales@coreptt.com. Registered telephone: (11) 9839-0601. Legal matters, privacy, integrity and security: legal@coreptt.com.

The PROVIDER is the legal entity responsible for the commitments it undertakes in the corePTT instruments. The CUSTOMER and the representatives of both parties will be identified in the applicable instrument, with authority to approve the scope and sign.

1 Proposal identification

Field	Completion
Proposal number	[complete]
Issue and validity	[dd/mm/yyyy] • valid until [dd/mm/yyyy]

Field	Completion
Commercial start and term	[dd/mm/yyyy hh:mm, Brasília] • [initial term]
Commercial renewal	automatic expressly accepted [] upon new acceptance [] not applicable []
Commercial renewal conditions	[complete term, amounts or valid rule, notice and nonrenewal notice period]
Previous trial reference	not applicable [] 7-day agreement No. [complete]

2 CUSTOMER

Field	Completion
Legal name	[complete]
CNPJ	[complete]
Address	[complete]
Representative	[complete]
Sales contact	[complete]
Technical contact	[complete]
Security contact	[complete]
Data protection officer or privacy contact	[complete]
Email for tax invoice	[complete]
Finance email	[complete]

3 PROVIDER

Field	Information
Legal name	COREPTT TECNOLOGIA LTDA
Trading name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand	corePTT
Sales and contracting	sales@coreptt.com

Field	Information
Registered telephone	(11) 9839-0601
Legal matters privacy and integrity	legal@coreptt.com
Representative and authority	[complete name, title and evidence of authority before signature]

4 Selected scope

Select	Module or service	Quantity and notes
☐	Users and licenses	[complete]
☐	Android application	[complete]
☐	iOS application	[complete]
☐	Web dispatch console	[complete]
☐	Voice and PTT groups	[complete]
☐	Voice recording	[complete]
☐	Video	[complete]
☐	Messages and files	[complete]
☐	Location and history	[complete]
☐	Geofences and alerts	[complete]
☐	DMR integration or gateway	[complete]
☐	API and integrations	[complete]
☐	Implementation and configuration	[complete]
☐	Training	[complete]
☐	Equipment	[complete]
☐	SIM cards and connectivity	[complete]
☐	Additional professional service	[complete]

5 Environment and architecture

Field	Definition
Environment type	shared ☐ dedicated ☐ installed at the CUSTOMER ☐ hybrid ☐

Field	Definition
Production	[complete]
Validation	included [] not included []
Hosting region	[complete]
Federated identity	no [] yes [] standard: [complete]
Administrative MFA	mandatory [] optional [] unsupported in the component []
Encryption and protocols	as specified in Technical Annex No. _____
Redundancy	[complete]
RTO and RPO	[complete]
User device and channel limits	[complete quantities, concurrent limits and overages]
Storage and capacity	[complete capacity and treatment of overages]

6 Implementation and acceptance

Stage	Responsible party	Date or criterion
Discovery and requirements	PROVIDER and CUSTOMER	[complete]
Configuration	PROVIDER	[complete]
Integrations and connectivity	_____	[complete]
Acceptance test	CUSTOMER	[complete]
Training	_____	[complete]
Go-live	PROVIDER and CUSTOMER	[complete]

Objective criteria, responsible parties and the acceptance deadline will be completed in the Technical Annex and the schedule of this Order. Commercial go-live will depend on a formal contract and documented acceptance; silence or use during the trial does not replace a signature or create a payment obligation.

7 Prices

Item	Quantity	Unit price	Frequency	Total
_____	_____	R\$ _____	_____	R\$ _____
_____	_____	R\$ _____	_____	R\$ _____
_____	_____	R\$ _____	_____	R\$ _____

Item	Quantity	Unit price	Frequency	Total
_____	_____	R\$ _____	_____	R\$ _____
_____	_____	R\$ _____	_____	R\$ _____

Condition	Definition
Implementation	R\$ [complete]
Monthly fee	R\$ [complete]
Equipment	R\$ [complete]
Authorized expenses	[complete]
Due date	[complete]
Payment method	[complete]
Adjustment index	IPCA [] other _____
Dispute period	_____ days
Currency taxes and breakdown	[complete currency, included taxes and itemized components]
Late payment charges	[percentages and criteria to be completed and accepted]
Notice and cure period	[method and period to be completed before commercial suspension]
First billing	[date and event triggering commercial billing; no retroactive charges for the trial]
Adjustment frequency	[complete according to the statutory minimum period]

8 Selected SLA

Select	Plan	Target	Coverage
[]	Essential	99.5 percent	business days from 8h to 18h
[]	Operational	99.9 percent	P1 24 by 7 and other priorities on business days
[]	Customized	_____	[complete]
[]	No contracted availability target	not contracted	support and diligence according to the accepted scope

Measured components: _____

P1 channel and escalation contacts: _____

Measurement points and interval: [complete]. Period and time zone: [complete]. Window and monthly limit for excluded maintenance: [complete]. Support channels, days and hours: [complete]. First response, update and workaround targets: [accepted SLA table or specific definition]. Credits: [accepted SLA table or specific rule]. All relevant fields will be validated before commercial activation.

9 Retention and privacy

Select the period by category and record the legal basis, purpose, responsible parties and transparency in the DPA. The 90-day retention period applies only when expressly selected and accepted. The content window is distinct from backup retention. Duplicate or conflicting settings in this Order will be reconciled before signature; no box will be presumed checked.

Category	Period or setting
Voice recordings	7 days ☐ 30 days ☐ 90 days ☐ 180 days ☐ other _____
Videos	7 days ☐ 30 days ☐ 90 days ☐ other _____
Messages and files	30 days ☐ 90 days ☐ 365 days ☐ other _____
Location	current ☐ history _____ days ☐ geofence ☐
Access logs	statutory minimum and an additional period of _____
Export after expiry	30 days ☐ 60 days ☐ other _____
Anticipated sensitive data	no ☐ yes ☐ description in the DPA ☐
Children or adolescents	not anticipated ☐ anticipated with safeguards ☐

10 Subprocessors and transfers

Field	Definition
List of subprocessors	attached ☐ page with version/date and retained copy ☐ ; reference: [complete]
Countries and regions	[complete]
International transfer	no ☐ yes ☐
Mechanism	adequacy ☐ ANPD standard contractual clauses ☐ other _____
DPA Annex C completed	yes ☐ not applicable ☐

11 Equipment

Item	Model and serial number	Arrangement	Warranty or return
_____	[complete]	sale [] rental [] gratuitous loan for use []	_____
_____	[complete]	sale [] rental [] gratuitous loan for use []	_____
_____	[complete]	sale [] rental [] gratuitous loan for use []	_____

12 Connectivity

Field	Definition
Authorized carrier	[complete]
Quantity and identification of SIM cards	[complete]
Technology and bands	[complete]
Allowance and speed	[complete]
Coverage and roaming	[complete]
Overage and blocking	[complete]
Party responsible for the telecommunications service	[complete]

13 Assumptions and exclusions

Infrastructure provided by the CUSTOMER: _____

Approved integrations and versions: _____

Expressly excluded items: _____

Accepted dependencies and risks: _____

14 Special conditions

15 Incorporated documents

Document	Version date and reference	Received and accepted
corePTT Enterprise Agreement	1.3 or other: _____ • date: [complete]	[]
Data Processing DPA	1.3 or other: _____ • date: [complete]	[]
Support and Availability SLA	1.3 or other: _____ • date: [complete]	[]
Terms of Use	1.3 or other: _____ • date: [complete]	[]
Acceptable Use Policy	1.3 or other: _____ • date: [complete]	[]
Technical Annex	No. _____ • date: [complete]	[]
List of subprocessors	date ____/____/____	[]
Privacy Policy	version [complete] • date [complete]	[]
Backup Retention and Deletion Policy	version [complete] • date [complete]	[]
Hosting and Management Policy	version [complete] • date [complete]	[]
7-day Evaluation Agreement	when applicable • revision 1.3 • 14/10/2026	[]

16 Validity and acceptance

This proposal remains valid until the date or for the period completed. Acceptance by a duly authorized representative confirms only the scope, prices, assumptions and documents identified in this version. All applicable fields must be completed or marked not applicable before signature; outstanding material matters prevent the corresponding activation. Reservations and modifications will take effect only if accepted by both Parties. Commercial activation requires a formal contract. Commercial renewal will follow only the option and conditions expressly accepted in this Order; the free evaluation neither renews automatically nor automatically converts into a paid plan. The signature will record authorship, integrity, version, date and time.

External documents form part of the relationship only if made available to the CUSTOMER before acceptance and identified by title, version and date. Future policies will not be incorporated automatically, and no revision will retroactively change a contract; contractual changes require a written amendment accepted by the parties, preserving mandatory rules.

Selected integrations and external components

Field	Contractual definition
Component or application	[complete]
Supplier and brand	[complete]

Field	Contractual definition
License and version	[complete]
Party responsible for contracting	PROVIDER [] CUSTOMER [] third party []
Shared data	[complete]
External SLA or support	[complete]
Known limitations	[complete]
Contingency plan	[complete]

Ownership of developments

Item	Definition
PROVIDER preexisting components	remain with the PROVIDER []
Third-party components	attached licenses []
Exclusive development	no [] yes [] attached scope []
Assignment of source code	not provided for [] provided for in a specific annex []
Use of the CUSTOMER brand	no [] authorized within the limits of the annex []

Development and customization services

Field	Contractual definition
Problem and objective	[complete]
Deliverables	[complete]
Assumptions and dependencies	[complete]
Milestones and schedule	[complete]
Acceptance criteria and deadline	[complete]
Maintenance and warranty	[complete]
Amount and billing method	[complete]
Change request	process/annex: [complete]

Hosting and management

Field	Contractual definition
Environment type	shared ☐ dedicated ☐ jointly managed ☐
Hosting provider and region	[complete]
Reserved resources	[complete]
Layers managed by the PROVIDER	[complete]
Layers managed by the CUSTOMER	[complete]
Maintenance window	[complete]
Monitoring and alerts	[complete]

Retention, backup and recovery

Field	Contractual definition
Operational content	period by category as specified in section 9; 90 days only when selected and accepted
Export or long-term archive	no ☐ yes ☐ description: _____
Backup frequency	[complete]
Backup retention	[complete]
RPO	not contracted ☐ target: [complete]
RTO	not contracted ☐ target: [complete]
Restoration test	[complete]
Exclusions	[complete]
Active deletion after commercial termination	[complete maximum period, responsible party and confirmation]
Residual purging after commercial termination	[complete maximum backup period, blocking and responsible party]

7-day free evaluation

The evaluation depends on its own agreement and the validated schedule below. It does not automatically receive the commercial SLA or retention of recordings for 90 days. The CUSTOMER will maintain contingency measures and will not rely exclusively on the trial for emergencies or critical operations. Formalization and continuity: sales@coreptt.com; legal matters, privacy and integrity: legal@coreptt.com. During the free trial, the CUSTOMER must perform or request the necessary exports before expiry. Without

a contract or legally necessary preservation, operational content will be deleted or anonymized within 30 calendar days after expiry; any residual backup copies will be purged within 90 days after expiry, with restricted access and without operational reuse. The periods will be validated against the architecture before signature. Statutory retention and the regular exercise of rights follow their own periods and purposes. The trial does not guarantee retention of recordings for 90 days or recovery of content already deleted.

Field	7-day free evaluation schedule
Applicability and reference	no [] yes []; separate agreement No. [complete], revision/date [complete]
Account or environment	[complete identification]
Activation and communication	[dd/mm/yyyy hh:mm] • Brasília time zone • email record [complete]
Expiry	[dd/mm/yyyy hh:mm] • 168 hours after the communicated activation
License and access	R\$ 0,00 • does not create a purchase obligation or retroactive charges for the trial
Limits	[complete users, devices, groups/channels, storage and capacity]
Features and integrations	[complete enabled features; recording yes/no; location yes/no]
Hosting and service providers	[complete hosting provider, country, region, subprocessors and international mechanism]
CUSTOMER responsible person	[complete name, title, email and technical contact]
Permitted data	fictitious [] anonymized [] authorized real data []; categories/basis/transparency in the DPA
Backup or recovery	no guarantee by default []; specific obligation accepted [] annex [complete]
Continuity or extension	no automatic renewal/conversion; free extension in writing; paid plan through an accepted proposal and a formal contract
Export before expiry	[complete responsible party, format and agreed support]; later access not guaranteed
Active deletion	within 30 calendar days after expiry; statutory exceptions and architecture validated before signature
Residual backup copies	purging within 90 days after expiry; no operational reuse; architecture validated before signature
Schedule validation	[responsible parties on both sides, date and written record before activation]

Document control

Field	Record
Document owner	COREPTT TECNOLOGIA LTDA

Field	Record
Coordination and legal review	Responsible person to be appointed by the PROVIDER before signature
Sales and contracting	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com
Revision and date	1.3 • 14 October 2026
Status	Draft for legal review

PROVIDER	CUSTOMER
COREPTT TECNOLOGIA LTDA	Legal name indicated in the Service Order
CNPJ 69.599.966/0001-93	CNPJ indicated in the Service Order
Representative name and title	Representative name and title
Electronic signature	Electronic signature



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Technical Annex on Features Compatibility Equipment and Testing

Controlled register of features, integrations, manufacturers, equipment and evidence

corePTT platform

Compliance and governance

Security and data protection

11

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 Technical Annex on Features Compatibility Equipment and Testing

Controlled register of features, integrations, manufacturers, equipment and evidence

PROVIDER	COREPTT TECNOLOGIA LTDA
Trading name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14/10/2026
Status	Draft for legal review
Sales channel	sales@coreptt.com (11) 9839-0601
Legal matters privacy and integrity	legal@coreptt.com

This document organizes corePTT technical statements and prevents catalog references, internal testing, regulatory approval and contractual commitments from being treated as equivalent.

This Technical Annex records features, integrations, equipment, versions and test evidence associated with corePTT. Merely mentioning a manufacturer or model does not mean that the item has been tested, made available, approved or included in a specific contract.

Company identification and version control

COREPTT TECNOLOGIA LTDA, trading name COREPTT TECNOLOGIA, registered with the CNPJ under 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, is the PROVIDER responsible for the offering and the commitments undertaken in this instrument.

Sales and contracting: sales@coreptt.com; telephone (11) 9839-0601. Legal matters, privacy and integrity: legal@coreptt.com. The CUSTOMER or evaluating organization will be identified in the specific instrument through a representative authorized to accept it.

This document is revision 1.3, dated 14/10/2026, and constitutes a draft for legal review. Its incorporation requires that it be made available and identified by title, version and date before acceptance. Changes in scope or obligations require the applicable records and acceptance; there will be no automatic incorporation of future versions or retroactive unilateral change.

Purpose and interpretation rules

Declared compatibility is limited to the recorded model, firmware, license, frequency band, configuration, topology and scenario. A change in any of these elements may require new validation. The Service Order identifies the items actually supplied to the CUSTOMER; in the free trial, only the accepted activation schedule authorizes the features and integrations being evaluated.

The term approved is reserved for regulatory approval granted by Anatel, where applicable, and must be accompanied by the corresponding number. Evaluations conducted by the PROVIDER will use the terms laboratory validated, field validated, compatible with qualifications, under validation, untested or unsupported.

References to 3GPP, MCPTT, MCVideo, MCDATA or MCX standards, radio protocols or certification programs may be published as implemented capabilities or compliance only when corresponding scope, version, evidence and validation exist. Gateway integration, an intention to develop or participation in a test does not equate to platform certification.

Controlled functional catalog

Group	Function	Status and notes
Communication	group call and individual call	to be recorded by plan and version
Emergency	alert, priority and emergency call	to be recorded by scenario
Dispatch	web console, groups and operational coordination	to be recorded by license
Location	position, history and geofence	depends on device and permissions
Evidence	voice recording and playback	depends on retention and CUSTOMER policy
Multimedia	video, image, message and file	depends on application, network and plan
Integration	DMR and PoC gateway	requires validation by system, model and version
Integration	API, webhook and connectors	according to the contracted technical scope
Administration	users, groups, profiles and multiple environments	according to permissions

Manufacturer and ecosystem references

Manufacturer	Ecosystems and reference names	Infrastructure examples	Publication rule
Hytera	DMR Tier II, DMR Tier III, XPT and HyTalk	HR106X, HR65X and DS-6250S	do not declare tested without a record

Caltta	DMR Conventional, DMR Trunking, IP Connection and eChat PoC	PR900, PR680 and TBS6000	do not declare tested without a record
Motorola Solutions	MOTOTRBO, IP Site Connect, Capacity Plus, Capacity Max and WAVE PTX	SLR 1000, SLR 5000 and SLR 8000	do not declare tested without a record

The names above are used for technical identification of the ecosystems. Commercial availability, representation, supply, licensing and compatibility must be confirmed for each proposal.

Equipment and repeater register

Manufacturer and model	Band and firmware	System and license	Location and date	Result and evidence
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Test environments and methodology

Tests may take place in the PROVIDER laboratory, a partner laboratory or the CUSTOMER environment, in accordance with authorization and a documented plan. This instrument does not declare a laboratory installation at a specific address. The report records the location actually used without disclosing a customer, topology, credentials, serial number or sensitive information without authorization.

The free evaluation lasts 7 calendar days, equivalent to 168 hours from activation and communication of access credentials. It does not include a commercial SLA or validation for exclusive use in an emergency or critical process. The CUSTOMER must maintain alternative communication and contingency measures. Upon expiry, continuity depends on an accepted proposal and a formal contract through sales@coreptt.com; there is no automatic renewal or conversion into a paid service.

Required field	Record
Test identifier	_____
General location	laboratory [] field [] CUSTOMER [] partner []
City and State	_____
Date and responsible parties	_____
Topology and connectivity	_____

Required field	Record
Models, serial numbers and firmware	_____
Licenses and settings	_____
Functions evaluated	_____
Result and restrictions	_____
Evidence	report ☐ logs ☐ photos ☐ screenshots ☐ protocol ☐
Anatel approval	No. _____ status _____
Platform and application version	_____
Approved scope and person responsible for acceptance	_____
Authorized recording and location	no ☐ yes ☐ limits and permissions: _____
Contingency plan	_____
Evaluation start and end	___/___/___ :__ to ___/___/___ :__ Brasília
Hosting and service providers	_____
Evidence of revalidation after a change	_____

Result criteria

Status	Use
Available	feature offered under the indicated plan and version
Laboratory validated	controlled test with identified evidence
Field validated	test in the described operational environment
Compatible with qualifications	works within the recorded limitations
Gateway or API integration	depends on the identified external component
Under validation	evaluation not yet completed
Untested	insufficient evidence for a public statement
Unsupported	use outside the current technical scope

Technical and third-party responsibility

The PROVIDER is responsible for the tests, integrations and its own components that it undertakes within the documented scenario. External updates, license changes, incompatible firmware, network failures or unauthorized modifications require assessment of cause, prevention and mitigation. The analysis will distinguish the platform, integration, equipment, connectivity and CUSTOMER environment, without excluding nonderogable statutory responsibilities.

Trademarks and independence

Hytera, Caltta, Motorola Solutions and the other trademarks mentioned belong to their respective owners. The references serve identification purposes. Validation conducted by the PROVIDER does not constitute manufacturer certification or endorsement, unless stated in writing. Third-party logos must not be used without authorization or an applicable brand guideline.

Reports, logs, photos and test screenshots must limit personal data to what is necessary. Recording and location will be evaluated only if enabled in the activation schedule, with permissions, information to data subjects and a legal basis defined by the CUSTOMER. Hosting, service providers and any international transfer mechanism will be identified before activation.

Document control

Field	Record
Editorial ownership and maintenance	COREPTT TECNOLOGIA LTDA
Person responsible for approval	Authorized representative to be identified at acceptance
Sales channel	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Development Customization and Integrations Annex

Rules for professional services custom solutions and change control

corePTT platform

Compliance and governance

Security and data protection

12

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 Development Customization and Integrations Annex

Rules for professional services custom solutions and change control

PROVIDER	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14/10/2026
Status	Draft for legal review
Sales channel	sales@coreptt.com (11) 9839-0601
Legal privacy and integrity	legal@coreptt.com

This annex converts integration and customization requests into verifiable scopes, with clearly identified acceptance criteria, responsibilities, intellectual property and dependencies.

This Annex governs the offering of integration, solution development and customization related to corePTT. It must be used with the applicable Enterprise Agreement, Order Form, DPA and SLA.

Company identification and version control

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with CNPJ under 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, is the PROVIDER responsible for the offering and the commitments undertaken in this instrument.

Sales and contracting: sales@coreptt.com; telephone (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. The CUSTOMER or evaluating organization shall be identified in the specific instrument by a representative authorized to accept it.

This document is revision 1.3, dated 14/10/2026, and is a draft for legal review. Incorporation requires that its title, version and date be made available and identified before acceptance. Changes to scope or obligations require the applicable record and acceptance; future versions shall not be incorporated automatically and no retroactive unilateral changes shall apply.

1 Purpose

The PROVIDER may perform professional services to adapt corePTT to the CUSTOMER's context, integrate systems, equipment and data, create modules or automations, and support deployment, migration and operation. Only items approved in a signed proposal are included in the scope.

The free evaluation license is separate from these professional services: it lasts 7 calendar days, equivalent to 168 hours from the notified activation, and does not automatically include development, customization, migration or commercial support. Additional services require a separate instrument, costs accepted in advance and authorized representatives. At the end of the trial, contracting must be formalized through sales@coreptt.com or (11) 9839-0601, without automatic conversion or retroactive charges for the free license.

2 Service types

Type	Examples	Contractual outcome
Discovery and architecture	requirements, processes, risks and technical design	report, scope or architecture
Configuration	profiles, groups, permissions, workflows and parameters	configured environment
Customization	screens, fields, visual identity, rules and reports	feature adapted to the CUSTOMER
Integration	API, webhook, gateway, DMR, PoC and enterprise systems	connector or integrated workflow
Development	module, service, dashboard, automation or application	deliverable defined in the proposal
Migration and deployment	loading, validation, training and go live	deployed environment
Assisted operation	monitoring, adjustments and initial support	contracted assistance period

3 Scope definition and approval

1. The CUSTOMER describes the objective, users, data, current process, restrictions and systems involved.
2. The PROVIDER analyzes feasibility, dependencies, security, privacy, licenses, capacity and technical risks.
3. The proposal identifies deliverables, exclusions, assumptions, schedule, price, billing milestones, acceptance criteria and period, infrastructure and responsible parties. Delays in required inputs and scope changes shall be recorded with their expected effects before additional work is performed.
4. Work begins after commercial approval, provision of the required inputs and identification of authorized representatives.
5. Subsequent changes follow change control and may affect timing, price, architecture, security and support.

4 CUSTOMER obligations

- provide complete requirements, truthful information, authorized access and a compatible test environment;
- appoint a technical lead and an acceptance authority empowered to make decisions and set priorities;
- obtain licenses, authorizations, legal bases and rights to the data, brands, content and systems it provides;
- validate integrations and deliveries within the period specified in the Order Form;
- report changes in manufacturer, version, firmware, network, API, policy, volume and process that affect the solution.

5 Delivery testing and acceptance

Each delivery shall be compared with the recorded acceptance criteria. The PROVIDER may use a development, validation or production environment, as specified in the deployment plan. The CUSTOMER must record any rejection objectively, with reproducible evidence and a link to the approved requirement.

A defect is a reproducible discrepancy between the delivery and the approved criterion. A new preference, an undocumented rule, an increase in volume, adaptation to an external update or a subsequent request is a scope change. Correction periods, warranty and support depend on the Order Form. Any deemed acceptance requires a specific clause accepted in advance, a reasonable period, objective criteria and an opportunity to identify discrepancies; it does not apply to acceptance of the free trial or create a contract through mere use.

6 Intellectual property and reuse

The PROVIDER and the respective rights holders retain rights to corePTT, preexisting components, libraries, methods, models, generic connectors, tools, knowledge and reusable improvements, within the limits of their ownership and licenses. The CUSTOMER retains its data, brands, content, proprietary rules and preexisting materials. Use of the CUSTOMER's confidential material in a reusable component requires specific authorization or effective removal of that material.

Customization does not imply exclusivity, assignment or delivery of source code. An assignment of rights or special license requires a written annex identifying the material, type, territory, term, remuneration, code and documentation. Free software and third party components remain subject to their respective rights holders' licenses.

7 Integrations and third parties

The PROVIDER is responsible for the connector, configuration and activities it undertakes. Operation may depend on an API, license, firmware, equipment, network, cloud or external policy. Third party changes may require updating, revalidation, replacement or a new contract. Reference to a manufacturer does not represent endorsement or partnership without a formal instrument.

8 Data protection and security

The project must apply purpose limitation, necessity, security and privacy by design. The Order Form and DPA must specify data, roles, instructions, integrations, subprocessors, environment, retention, international transfers and incident and deletion procedures.

Sensitive personal data and data concerning children or adolescents are excluded from the free trial, unless specifically agreed in advance and the legal requirements are met. Commercial acceptance does not replace information to data subjects or the legal basis for processing. Communications content shall not

be used for advertising, sale to third parties or training AI models without a specific agreement and an appropriate legal basis.

9 Infrastructure and operation

The solution may use a shared or dedicated environment. The PROVIDER administers only the contracted layers and documents responsibilities for the application, database, operating system, network, cloud, terminals, licenses, backup and security. Capacity, availability, RPO, RTO and retention depend on the approved plan.

The environment, country, provider, subprocessors and applicable mechanism for any international transfer shall be disclosed and validated before processing. During free evaluation, subsequent access is not guaranteed; export and migration must be agreed before expiry. Without a contract or lawful preservation, operational content shall be deleted or anonymized within 30 days after the end, and residual backups purged within 90 days after the end, with access blocked for normal use. These periods must be validated against the architecture before signing.

10 Specific request details

Field	Entry
CUSTOMER and project	
Business objective	
Deliverables	
Integrations and versions	
Data and environments	
Exclusions and assumptions	
Schedule and milestones	
Acceptance criteria and period	
Intellectual property	
Support and maintenance	
Price and billing	
Responsible parties and approval authority levels	
Environment country provider and subprocessors	
CUSTOMER legal basis and permissions	
Risks security and contingency	

Field	Entry
Change procedure and budget	_____
Export deletion and backups	_____

11 Liability and changes

Each party is responsible for its acts, information, access, licenses and obligations. Liability limitations follow the Enterprise Agreement and do not exclude nonwaivable statutory duties. No preliminary estimate replaces the approved proposal. Changes must be authorized by identified representatives and recorded before execution.

The parties shall observe confidentiality and integrity duties; improper advantages, fraud and use of integrations to circumvent authorizations, approval authority levels or internal controls are prohibited. Suspected irregularities and privacy matters shall be referred to legal@coreptt.com; good faith reports shall be handled without retaliation. Audits require a proportionate scope agreed in advance, with protection for third party data and trade secrets.

Document control

Field	Record
Editorial ownership and maintenance	COREPTT TECNOLOGIA LTDA
Approval authority	Authorized representative to be identified upon acceptance
Sales channel	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com

PROVIDER	CUSTOMER
COREPTT TECNOLOGIA LTDA	Registered company name stated in the Order Form
CNPJ 69.599.966/0001-93	CNPJ stated in the Order Form
Representative name and title	Representative name and title
Electronic signature	Electronic signature



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

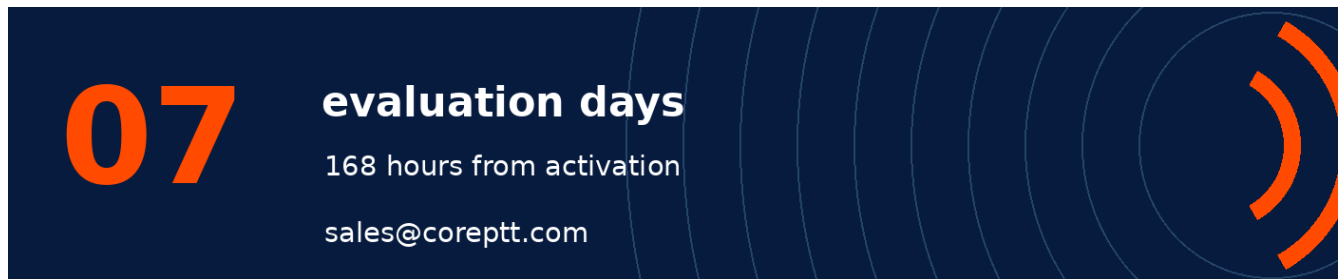
corePTT 07 Day Evaluation and Testing Agreement

Free evaluation license for public and private organizations

corePTT platform

Compliance and governance

Security and data protection



COREPTT TECNOLOGIA LTDA

CNPJ 69.599.966/0001-93 • Campinas SP

Revision 1.3 | 14 October 2026

DRAFT FOR LEGAL REVIEW

corePTT 07 Day Evaluation and Testing Agreement

Free evaluation license for public and private organizations

PROVIDER	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14/10/2026
Status	Draft for legal review
Sales channel	sales@coreptt.com (11) 9839-0601
Legal privacy and integrity	legal@coreptt.com

This Agreement governs the free corePTT evaluation license for 7 days, with resource limits, responsibilities, security, data protection, integrity and termination without automatic conversion to a paid plan.

The PROVIDER grants the evaluating organization a nonexclusive, nontransferable license limited to internal evaluation of the features enabled in the accepted schedule. The free trial has a value of R\$ 0,00 and lasts 7 calendar days, equivalent to 168 hours from the notified activation. It does not transfer intellectual property, exclusivity, resale rights or rights to public use of the brand or a commercial reference.

Company identification and version control

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with CNPJ under 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, is the PROVIDER responsible for the offering and the commitments undertaken in this instrument.

Sales and contracting: sales@coreptt.com; telephone (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. The CUSTOMER or evaluating organization shall be identified in the specific instrument by a representative authorized to accept it.

This document is revision 1.3, dated 14/10/2026, and is a draft for legal review. Incorporation requires that its title, version and date be made available and identified before acceptance. Changes to scope or obligations require the applicable record and acceptance; future versions shall not be incorporated automatically and no retroactive unilateral changes shall apply.

1 Evaluation identification

Field	Entry
Evaluating organization and nature	_____
CNPJ and full address	_____
Representative name title and authority	_____
Organization email and telephone	_____
Technical lead and contact	_____
Environment or account identification	_____
Purpose of the evaluation	_____
Start of notified activation	___/___/___ __:___ Brasília time zone
End after 168 hours	___/___/___ __:___ Brasília time zone
Users devices groups and channels	_____
Storage and other limits	_____
Enabled features	_____
Authorized integrations models and versions	_____
Audio and video recording	no ☐ yes ☐ permissions: _____
Geolocation	no ☐ yes ☐ permissions: _____
Alternative communication and contingency	_____

2 Purpose and temporary nature

The evaluation enables the organization to explore features, validate suitability, conduct a proof of concept and produce evidence for an internal decision. It does not replace public emergency services or a formal procurement process. The evaluating organization must maintain alternative communication and contingency arrangements, without relying exclusively on the trial for emergencies, rescue, people's safety or control of critical processes.

The period begins upon activation and communication of access credentials, not upon mere signing. The schedule must contain the start and end with the time and Brasília time zone, covering 168 hours. A free extension requires express written approval with a new end date. There is no automatic renewal, automatic conversion to a paid plan, retroactive charge for the free license or purchase obligation.

Internet, mobile data, equipment, external licenses and the evaluating organization's infrastructure are its responsibility. Additional services or equipment loans require a separate instrument with costs accepted in advance. Continuation after the trial requires an accepted proposal and formal contract specifying licenses, amounts, payment, support, service levels and data processing; mere contact with sales does not extend access or guarantee preservation of content.

To formalize use after the trial, sales shall be contacted through sales@coreptt.com or (11) 9839-0601. Any expiry reminder does not change the stated end date, and its absence does not extend the evaluation.

3 Features and limitations

- functions, users, devices, groups/channels, storage capacity and integrations shall be limited to those enabled in the activation schedule; features not listed are excluded from the trial;
- the environment may undergo maintenance, restart, updating, preventive limitations or corrections, with foreseeable impacts communicated where possible;
- compatibility applies only to the models, versions, licenses and configurations actually recorded;
- there is no commercial commitment regarding availability, coverage, latency, 24 hour support, SLA, RPO, RTO, backup or restoration; an additional obligation exists only if expressly identified and accepted;
- the Terms of Use, Acceptable Use Policy and other policies form part of the evaluation only when made available before acceptance and identified by title, version and date; future versions are not incorporated automatically.

4 Use by private organizations

The private organization shall appoint a responsible administrator, maintain correct registration details, restrict access to authorized persons, guide users and protect individual passwords and devices. It must obtain the necessary licenses, authorizations and legal grounds and prefer fictitious or effectively anonymized data where sufficient. Suspected intrusion, device loss or misuse shall be reported immediately.

Unlawful use, fraud, harassment, infringement of third party rights, sharing or reselling access, attempted access to other accounts, malicious code, exploitation of vulnerabilities, reverse engineering outside legally permitted circumstances and load, penetration or security testing without written authorization are prohibited. Connections to radios, networks or external systems require the applicable authorizations and licenses.

5 Use by public bodies and entities

The public body must state its authority, public purpose, legal basis, responsible persons and information classification, and observe its security, procurement, transparency, archiving and data protection procedures. The trial does not anticipate an award, contract, exclusivity or budget commitment.

Data relating to public security, national defense, State security, investigation or prosecution of criminal offenses must not be entered without a specific instrument, public oversight and legal and security validation compatible with the applicable regime.

6 Personal data and trial content

For user, communications and location data processed under the evaluating organization's instructions, that organization shall act as controller and the PROVIDER as processor. For commercial registration, contract management, fraud prevention and its own obligations, the PROVIDER may act as an independent controller according to the actual purposes. Each party is responsible for the processing under its responsibility and shall cooperate in responding to data subjects.

Processing may cover name, email, telephone, identifiers and access and usage records; voice, video, messages and location only when enabled. The purposes are to provide the trial, administer access, provide support and protect and evaluate the environment. The evaluating organization shall determine the legal basis and inform data subjects in advance about monitoring, recording, location, access and periods. This acceptance does not constitute blanket consent. Sensitive data, including biometrics, data concerning children or adolescents and confidential or classified content are excluded from the trial, unless specifically agreed in advance, with safeguards and the relevant legal and security validation.

The PROVIDER shall follow lawful and documented instructions, limit access to necessary persons and adopt proportionate controls, including permissions management, credential protection and recording of relevant events. It shall not use communications content for advertising, sale to third parties or training AI models without a specific agreement and an appropriate legal basis.

The list of hosting and support service providers, the environment, processing countries and any international transfer and its mechanism shall be disclosed before activation. Service providers shall have access only to what is necessary and be subject to confidentiality and data protection obligations. Privacy matters and data subject requests shall be referred to legal@coreptt.com.

7 Termination export and deletion

At the end of 168 hours, the license expires and access may be suspended, including communications, dispatch, location and access to recordings. Before the end, the evaluating organization shall request or perform exports it wishes to retain using the available formats and features. Subsequent access, export or recovery is not guaranteed; export support and any migration must be agreed before expiry.

Without a contract or lawful preservation request, operational content shall be deleted or anonymized within 30 calendar days after the end. Residual backups, if any, shall be purged within 90 days after the end and shall not be reused for operational purposes. These periods shall be validated against the environment's architecture before signing. Records subject to statutory retention or necessary for the regular exercise of rights may be retained for the applicable period, with restricted access and a limited purpose.

8 Relationship with 90 day retention

Commercial retention of recordings for up to 90 days, where expressly contracted, is separate from the free evaluation and does not extend it. Subsequent contracting and migration require approval and actual data availability; they do not ensure recovery of content already deleted. The production environment shall follow the accepted Order Form, DPA and policy.

9 Security support and incidents

The PROVIDER shall maintain reasonable security measures and manage the layers it undertakes. Initial support shall be requested through sales@coreptt.com for referral to the responsible team, subject to availability and the accepted scope. A party identifying an incident involving personal data shall notify the other without undue delay, providing available information and updates. The controller shall assess and make notifications to the ANPD and data subjects when required, within statutory deadlines; the processor shall cooperate, without excluding each party's own obligations. A material interruption attributable to the platform may justify an extension if agreed in writing.

10 Specific conditions schedule

Item	Condition
Real personal data	no ☐ yes ☐ categories/legal basis: _____

Item	Condition
Sensitive data data concerning children and confidential data	Excluded from the trial unless a specific prior agreement is identified: _____
Hosting provider and region	_____
Processing countries and subprocessors	_____
International transfer and mechanism	no ☐ yes ☐ validated mechanism: _____
Expressly agreed backup	no ☐ yes ☐ scope/frequency: _____
Export before expiry	no ☐ yes ☐ format/responsible person: _____
Support during the trial	sales@coreptt.com conditions and hours: _____
Operational deletion after the end	within 30 days architecture validation: _____
Backup purge after the end	within 90 days architecture validation: _____
Party responsible for deletion	PROVIDER for managed layers; organization for exports
Authorized express extension	no ☐ yes ☐ until: ____/____/____ __:____
Incorporated instruments	title, version and date: _____
Acceptance of schedules and activation	representatives, version, date and confirmation: _____

11 Acceptance and precedence

Before activation, the parties shall validate this Agreement and its schedules through authorized representatives, recording the version, authorship, integrity, date and time of physical or electronic acceptance. Electronic signatures shall observe the requirements applicable to the accepted method. Mere use does not replace authorized acceptance or create a paid contract. Accepted external instruments must be identified by title, version and date; discrepancies shall be resolved by written agreement, subject to mandatory rules.

12 Confidentiality and intellectual property

Each party shall protect nonpublic information received in connection with the trial, including credentials, configurations, proposals and operational data, restricting access to necessary persons subject to confidentiality. The duty continues for 3 years after the end; trade secrets and personal data remain protected according to their nature and the law. Information demonstrably public, legitimately already known or received from a third party without breach is excluded. Mandatory disclosure shall be limited and notified where permitted. The platform, code, brands and documentation belong to their respective rights holders; the organization's data remain subject to its rights and those of its rights holders.

13 Integrity and governance

The parties shall comply with applicable legislation and anticorruption rules, including Law No. 12.846/2013 where applicable. Improper advantages, fraud, unlawful favoritism and use of the trial to circumvent purchasing, approval authority levels and internal controls are prohibited. Each party shall appoint a responsible person; changes to scope, resources and duration require documented approval. Governance shall include permissions control and revocation, approval records and evaluation of results. Audits require a proportionate scope agreed in advance, with protection for third party data, confidentiality and security, without unrestricted access to infrastructure or source code. Irregularities may be reported to legal@coreptt.com, with restricted access and without retaliation against good faith reports; certifications or technical compliance shall not be claimed without evidence.

14 Suspension termination and liability

The organization may end the trial by written notice without a penalty or charge for the free license. The PROVIDER may suspend or terminate access for unlawful use, material breach, security risk or an authority's order, stating the reason where permitted and allowing correction where compatible with the risk; urgent measures may be immediate. Each party is responsible for damages it causes according to its conduct, causation and the law. The free nature of the trial does not exclude security, data protection, good faith or nonwaivable liabilities, nor does it exempt willful misconduct or gross negligence. Internet, power and device failures and force majeure shall be assessed according to their cause and reasonable prevention and mitigation measures.

15 Final provisions and signatures

Brazilian law applies. The parties shall seek an agreed solution; the courts of the Judicial District of Campinas/SP are selected, subject to mandatory statutory jurisdiction and consumer protection where applicable. Tolerance does not constitute a waiver and partial invalidity does not affect the remaining provisions. After the end, confidentiality, data protection, intellectual property and liability continue for the applicable periods. The parties declare that they understand the duration, free nature and termination without automatic conversion to a paid plan and shall validate the schedules before signing.

Place and date: _____

Document control

Field	Record
Editorial ownership and maintenance	COREPTT TECNOLOGIA LTDA
Approval authority	Authorized representative to be identified upon acceptance
Sales channel	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com

PROVIDER	EVALUATING ORGANIZATION
COREPTT TECNOLOGIA LTDA	Registered company name: _____
CNPJ 69.599.966/0001-93	CNPJ: _____
Representative and title: _____	Representative and title: _____
Signature: _____	Signature: _____

corePTT Backup Retention and Deletion Policy

Rules for continuity restoration operational retention and secure disposal

corePTT platform

Compliance and governance

Security and data protection

14

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 Backup Retention and Deletion Policy

Rules for continuity restoration operational retention and secure disposal

PROVIDER	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14/10/2026
Status	Draft for legal review
Sales channel	sales@coreptt.com (11) 9839-0601
Legal privacy and integrity	legal@coreptt.com

This policy distinguishes contracted operational retention, recovery copies and deletion after termination. Retention of recordings for up to 90 days requires an express contract; the free 7 day trial has its own period and does not guarantee that window.

This Policy describes retention of operational content, the purpose of backups, restoration conditions and data deletion in corePTT environments managed by the PROVIDER.

Company identification and version control

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with CNPJ under 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, is the PROVIDER responsible for the offering and the commitments undertaken in this instrument.

Sales and contracting: sales@coreptt.com; telephone (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. The CUSTOMER or evaluating organization shall be identified in the specific instrument by a representative authorized to accept it.

This document is revision 1.3, dated 14/10/2026, and is a draft for legal review. Incorporation requires that its title, version and date be made available and identified before acceptance. Changes to scope or obligations require the applicable record and acceptance; future versions shall not be incorporated automatically and no retroactive unilateral changes shall apply.

1 Scope

The Policy applies to shared, dedicated and evaluation environments administered by the PROVIDER. The actual configuration depends on the plan, Order Form, DPA, architecture and CUSTOMER obligations. Resources maintained exclusively by the CUSTOMER follow its policies.

2 Concepts

Concept	Meaning
Operational retention	time during which content remains available in normal use
Backup	protected copy for environment recovery or continuity
Archive	long term storage for consultation, evidence or preservation
RPO	target recovery point and estimated maximum loss
RTO	target time for service recovery
Restoration	recovery of an eligible set from an available copy
Deletion	logical deletion and technical expiry according to the applicable cycle

3 Contracted operational retention

In commercial environments where expressly contracted, audio and video recordings may remain available for up to 90 calendar days in a rolling window, according to the limits and scope of the Order Form. Messages, files, location history and other categories shall have their own periods recorded by purpose. Once a category's period expires, its content becomes eligible for automatic deletion and may cease to be available for consultation without individual notice. This policy does not ensure a 90 day window in the free trial.

A period longer than 90 days for recordings requires separate negotiation, an estimate of volume, capacity, cost, security, purpose, legal basis and documentation in the Order Form. Archiving, recurring export, immutable storage or legal preservation shall be commitments only if expressly identified and validated.

4 Categories with their own periods

The 90 day window does not replace periods necessary for registration, billing, taxes, contracts, access records, authentication, security, support tickets, incidents, data subject rights, auditing or the regular exercise of rights. These data shall be retained according to purpose, necessity and the applicable obligation, with restricted access.

5 Backup is not an archive

Backups exist for technical recovery and continuity. They do not guarantee a complete history, restoration of an individual item, 90 day retention, immutability or immediate recovery. Each commitment depends on expressly contracted frequency, scope, retention, RPO, RTO and testing.

6 Backup plan

Field	Contracted configuration
Environment and components	_____
Included data	_____

Field	Contracted configuration
Excluded data	_____
Frequency	_____
Copy retention	_____
Location and provider	_____
Encryption and access	_____
RPO	not contracted [] target: _____
RTO	not contracted [] target: _____
Restoration test	_____
Periods by operational category	_____
Subprocessors and processing countries	_____
International transfer mechanism	not applicable [] mechanism: _____
Active data deletion after termination	_____
Backup purge after termination	_____
Deletions reapplied during restoration	_____
Technical validation and responsible person	_____

7 Operation and restoration tests

The PROVIDER monitors the execution of routines under its management, handles alerts and records material failures. Restoration tests shall be performed at the contracted frequency, in a controlled environment and with data protection. A test result demonstrates recoverability in the assessed scenario and does not eliminate risks.

8 Restoration request

The CUSTOMER shall submit an authorized support ticket stating the environment, period, subject and impact. The PROVIDER shall assess the available copy, integrity, conflict with current data, security and timing. Restoration may require a maintenance window, an alternative environment and validation; where not included in the plan, it shall require a quotation accepted in advance, without automatic charges. The procedure must preserve deletions and restrictions already applied to the data.

9 Usual exclusions

- data or files not included in the backup plan;

- content deleted before the first eligible copy;
- devices, networks, accounts or repositories maintained exclusively by the CUSTOMER;
- third party applications and services without a contracted export or copying mechanism;
- development or evaluation environments without express provision for backups;
- loss after the available recovery point.

10 Deletion and expiry of copies

At the end of the purpose or contract, active data shall be returned, deleted or anonymized according to the period and lawful instructions in the applicable instrument. Migration or export must be agreed before termination and does not guarantee recovery of content already deleted. In protected backups, granular changes may be impracticable or compromise integrity; in that case, the data shall remain blocked from normal use until purged within the documented period. If technical restoration is necessary, deletions and restrictions shall be reapplied before release for operational use.

Exceptional retention may occur for a legal or regulatory obligation, the regular exercise of rights, a valid order, an incident or a purpose permitted by the LGPD. The exception must be limited, documented and protected.

11 Evaluation environments

Free evaluation environments last 7 calendar days, equivalent to 168 hours from the notified activation, without guaranteed backup or restoration unless a specific commitment is accepted. At the end, the license expires and access may be suspended, without guaranteed subsequent consultation. Export must be requested or performed before expiry using the available features. Without a contract or lawful preservation, operational content shall be deleted or anonymized within 30 calendar days after the end and residual backups purged within 90 days after the end, blocked from ordinary use and without reuse for new purposes. These periods must be validated against the architecture before signing.

There is no automatic renewal, automatic conversion to a paid plan or retroactive charge for the free license. An extension requires express written approval. Continuation requires an accepted proposal and formal contract through sales@coreptt.com or (11) 9839-0601; contact with sales does not guarantee preservation or recovery. Minimum records for statutory retention and the regular exercise of rights may be retained with restricted access and a limited purpose.

12 Responsibilities

Party	Main responsibilities
PROVIDER	perform and monitor contracted routines, restrict access, handle failures and conduct authorized restoration
CUSTOMER	classify data, define retention, export when necessary, control users and validate restorations
Infrastructure provider	operate the infrastructure or service layer specified in its own commitments

13 Data protection and references

Retention and deletion observe purpose limitation, necessity, transparency, security and accountability. Termination of processing and retention circumstances follow, among others, Articles 15 and 16 of the LGPD; records, instructions and security measures follow Articles 37, 39 and 46 to 49.

The plan must identify the environment, storage countries, provider, subprocessors, access and mechanism for any international transfer before activation. An incident involving personal data shall be notified between the parties without undue delay; the controller shall assess statutory notifications with the processor's cooperation. Privacy and deletion requests shall be directed to legal@coreptt.com, with verification of their legitimacy and each party's authority.

Document control

Field	Record
Editorial ownership and maintenance	COREPTT TECNOLOGIA LTDA
Approval authority	Authorized representative to be identified upon acceptance
Sales channel	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Hosting and Server Management Policy

Shared and dedicated environments and operational responsibilities

corePTT platform

Compliance and governance

Security and data protection

15

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 Hosting and Server Management Policy

Shared and dedicated environments and operational responsibilities

PROVIDER	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14/10/2026
Status	Draft for legal review
Sales channel	sales@coreptt.com (11) 9839-0601
Legal privacy and integrity	legal@coreptt.com

This policy defines how the PROVIDER administers the layers it undertakes, distinguishes shared and dedicated environments and documents CUSTOMER and service provider responsibilities. The free trial follows its own duration and conditions, separate from commercial service levels.

This Policy describes corePTT hosting models and the server and technical component management responsibilities undertaken by the PROVIDER.

Company identification and version control

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with CNPJ under 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, is the PROVIDER responsible for the offering and the commitments undertaken in this instrument.

Sales and contracting: sales@coreptt.com; telephone (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. The CUSTOMER or evaluating organization shall be identified in the specific instrument by a representative authorized to accept it.

This document is revision 1.3, dated 14/10/2026, and is a draft for legal review. Incorporation requires that its title, version and date be made available and identified before acceptance. Changes to scope or obligations require the applicable record and acceptance; future versions shall not be incorporated automatically and no retroactive unilateral changes shall apply.

1 Environment models

Model	Characteristics	Point to consider
-------	-----------------	-------------------

Shared	common resources with logical segregation between CUSTOMERS	does not mean an exclusive physical machine
Dedicated	listed resources reserved for the CUSTOMER	network, control or cloud services may remain shared
Co-managed	responsibilities divided between the PROVIDER and the CUSTOMER	an access and change matrix is mandatory
In the CUSTOMER's environment	infrastructure supplied or contracted by the CUSTOMER	the PROVIDER manages only the specified layers
Evaluation	temporary free environment for 7 calendar days and 168 hours from the notified activation	without guaranteed commercial SLA, production, backup or restoration, unless specifically committed

2 Service managed by the PROVIDER

When contracted as a managed service, the PROVIDER's service may cover provisioning, secure configuration, administrative control, updating, observability, capacity, backup, restoration, maintenance, incident response and deactivation. The specific extent shall be defined by layer in the accepted schedule and instrument; items not included do not constitute a commercial commitment.

3 Responsibility matrix

Layer or activity	PROVIDER	CUSTOMER or third party
Datacenter or physical cloud infrastructure	coordinates supplier when included	provider operates its infrastructure
Virtual machine or server	manages when contracted	CUSTOMER approves capacity and cost
Operating system	configures and updates when included	CUSTOMER discloses dependencies and windows
corePTT database and application	operates, monitors and maintains	CUSTOMER administers usage and data
Integrations	maintains contracted connectors	external rights holder maintains API, license and service
User network and internet	supports diagnosis	CUSTOMER and telecommunications operator maintain connectivity
Terminals and radios	supports models within scope	CUSTOMER protects, updates and provides
Identities and permissions	provides administrative controls	CUSTOMER authorizes users and reviews access

4 Shared infrastructure

The PROVIDER adopts logical segregation, permissions, tenant identification and controls proportionate to risk. Capacity is managed on an aggregate basis and may be adjusted to maintain stability. Requirements for physical isolation, an exclusive key, a private network or a specific region must be contracted.

5 Dedicated infrastructure

The dedicated designation applies only to the listed resources. It does not automatically imply exclusive physical hardware, an exclusive team, an exclusive connection or the absence of shared provider services. Sizing, redundancy, licenses, region, addressing and administrative access must be recorded in the Order Form.

6 Security and administrative access

- privileged access must be individual, restricted by role and revoked when no longer necessary;
- credentials and secrets must be protected and must not be shared through insecure channels;
- material changes must have authorization, a record and a plan compatible with the risk;
- vulnerabilities and updates shall be handled according to criticality, compatibility and the operational window;
- logs and evidence shall have restricted access and retention appropriate to the purpose and contract.

7 Updating and maintenance

The PROVIDER shall plan updates to managed layers and may perform emergency fixes to reduce a material risk, recording the intervention and communicating foreseeable impacts where possible. Scheduled interventions shall follow the accepted commercial SLA and window where these exist. During the trial, maintenance does not create an SLA or 24 hour service. The CUSTOMER shall participate in testing integrations, firmware and processes dependent on the version.

8 Monitoring and capacity

Metrics, alerts, limits and monitoring hours depend on the plan. The PROVIDER shall handle alerts from the managed layer and propose expansion when there is a trend toward saturation. Increases in users, traffic, storage, integrations or retention may require resizing and a quotation accepted in advance; additional capacity shall not be charged automatically.

9 Backup retention and recovery

The Backup Retention and Deletion Policy supplements this document if identified and accepted during contracting. Retention of recordings for up to 90 days is a commercial commitment only where expressly contracted; other categories have their own periods. Copying frequency, backup retention, testing, RPO, RTO and restoration constitute commitments only when defined in the plan or Order Form. The free evaluation does not guarantee these features.

10 Third parties and subprocessors

The PROVIDER may use cloud, datacenter, communications, monitoring and security providers with the minimum necessary access and confidentiality and data protection obligations. It is responsible for selection, instructions, configuration and supervision compatible with the service it undertakes; division of layers does not exclude its legal or contractual obligations. The list of service providers and subprocessors, the environment, processing countries and mechanism for any international transfer shall be disclosed and

validated before activation in accordance with the DPA and applicable legislation. This policy does not claim certification, datacenter tier or technical compliance without specific substantiation.

11 Incidents and continuity

The PROVIDER shall perform triage, containment, recovery and communication within the layers it undertakes according to its role and severity. The CUSTOMER and service providers shall cooperate and preserve evidence. An incident involving personal data shall be notified between the parties without undue delay, with available information and updates; the controller shall assess notifications to the authority and data subjects when required, within statutory deadlines, with the processor's cooperation and without excluding their own obligations. Commercial contingency, redundancy and disaster recovery depend on the contracted design; during the trial, the CUSTOMER shall maintain its own alternative means.

12 Termination and transition

Upon termination, the PROVIDER shall deactivate access and resources under its management and return, delete or anonymize data according to accepted instruments and lawful instructions. Export, portability, migration and assistance must be agreed before termination; additional services shall require a quotation accepted in advance. Subsequent dashboard access and recovery of deleted content are not guaranteed.

In the free trial of 7 calendar days, equivalent to 168 hours from the notified activation, there is no automatic renewal or conversion to a paid plan. Continuation requires an accepted proposal and formal contract through sales@coreptt.com or (11) 9839-0601. Without a contract or lawful preservation, operational content shall be deleted or anonymized within 30 days after the end and residual backups purged within 90 days after the end, without operational reuse; the periods must be validated against the architecture before signing. Minimum records for statutory retention may remain with restricted access and a limited purpose.

13 Environment schedule

Field	Definition
Model	shared [] dedicated [] co-managed [] CUSTOMER [] evaluation []
Provider and region	_____
Resources and capacity	_____
Layers managed by the PROVIDER	_____
Layers outside scope	_____
Administrative access	_____
Monitoring	_____
Maintenance window	_____
Backup RPO and RTO	_____

Field	Definition
Retention of recordings and other categories	contracted period by category and limit: _____
Incident contacts	_____
Processing countries and subprocessors	_____
International transfer and mechanism	no ☐ yes ☐ validated mechanism: _____
Versions and resource limits	_____
Contingency and prior export	_____
Termination and deletion periods	_____
Architecture and persons responsible for validation	_____

14 Changes and precedence

A change in model, provider, region, capacity, retention or responsibility requires a risk assessment, a record and the relevant approvals; commercial impacts require acceptance. The Order Form defines the commercial environment, the SLA its service levels, the DPA personal data and the Enterprise Agreement the general rules. During the free evaluation, the accepted 07 Day Evaluation Agreement and activation schedule prevail for their specific scope. All incorporated instruments shall be identified by title, version and date before acceptance, without retroactive unilateral changes.

Document control

Field	Record
Editorial ownership and maintenance	COREPTT TECNOLOGIA LTDA
Approval authority	Authorized representative to be identified upon acceptance
Sales channel	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com



Push-to-talk solution

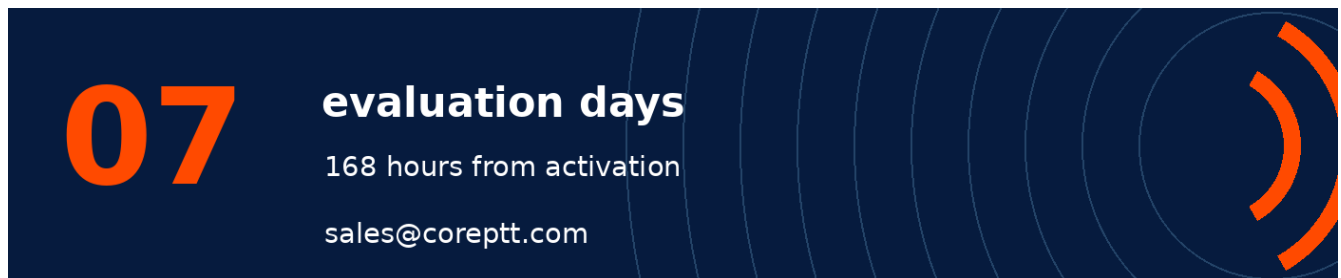
CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT free trial agreement

Temporary evaluation licence for 7 days

corePTT platform

Compliance and governance
Security and data protection



COREPTT TECNOLOGIA LTDA

CNPJ 69.599.966/0001-93 • Campinas SP

Revision 1.3 | 14 October 2026

DRAFT FOR LEGAL REVIEW

corePTT free trial agreement

Temporary evaluation licence for 7 days

This agreement governs the business evaluation of the corePTT platform under a free, temporary licence, with rules on security, data protection, compliance and governance. Access ends when the period expires, unless a formal service agreement is entered into or an extension is expressly approved in writing.

1 Parties

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, represented herein by its legal representative identified below.

EVALUATING CUSTOMER: [legal name], CNPJ [complete], with its registered office at [full address], represented by [name and position], email [complete], hereinafter CUSTOMER. The parties declare that their representatives are authorised to enter into this agreement.

2 Trial activation schedule

Environment or account identification: [complete].

CUSTOMER technical contact and contact details: [complete].

Start: [dd/mm/yyyy, hh:mm]. End: [dd/mm/yyyy, hh:mm]. Time zone: Brasília.

Duration: 7 calendar days, equivalent to 168 hours from activation notified to the CUSTOMER.

Limits: [number of users], [devices], [groups/channels] and [storage].

Enabled features and authorised integrations: [describe].

Audio/video recording: [yes/no]. Geolocation: [yes/no].

Hosting environment, country and service providers involved: [complete before activation].

Both parties must complete and validate the schedule before activation. The PROVIDER will confirm the dates and access details by email. Any feature not identified as enabled is outside the trial scope; any change requires a written record.

3 Purpose and free access

3.1 The PROVIDER grants a non-exclusive, non-transferable licence limited to internal evaluation of the enabled features. The trial allows technical and operational suitability to be assessed, without transferring intellectual property, exclusivity or resale rights.

3.2 The licence and access provided under this agreement have a value of R\$ 0,00. Internet, mobile data, equipment and CUSTOMER infrastructure are the CUSTOMER's responsibility. Additional services and equipment loans require a separate agreement, with costs accepted in advance.

4 Term and contracting after the trial

4.1 The term does not begin upon signature alone: it begins upon activation and notification of access details, as set out in the schedule. The PROVIDER will seek to send a reminder before expiry; failure to send it does not alter the notified end date.

4.2 At the end of the 168 hours, the licence expires and access may be suspended, including communications, dispatch, location and viewing of recordings. The CUSTOMER must plan continuity using its own means and arrange any necessary exports before the trial ends.

4.3 To formalise and maintain use, the CUSTOMER must contact the sales team at sales@coreptt.com or by telephone on (11) 9839-0601, as recorded in the corporate registration.

4.4 Continued use requires an accepted commercial proposal and a formal service agreement defining licences, charges, payment, support, service levels and applicable data processing. Contacting sales alone does not extend the trial or guarantee continued access or preservation of data.

4.5 There will be no automatic renewal, automatic conversion to a paid plan, retroactive charge for the trial or obligation to purchase. Any free extension requires express written approval specifying a new end date.

5 CUSTOMER obligations and acceptable use

5.1 The CUSTOMER will appoint a responsible administrator, keep its registration details accurate, limit access to authorised persons and instruct its users. It must use individual, secure passwords, protect devices and immediately report loss, suspected intrusion or misuse.

5.2 The following are prohibited: unlawful use; fraud; harassment; distribution of illegal content; infringement of third-party rights; sharing or reselling access; attempts to access other accounts; introduction of malicious code; exploitation of vulnerabilities; reverse engineering outside legally permitted cases; and load, penetration or security testing without written authorisation.

5.3 The CUSTOMER is responsible for its settings, network, connectivity, device compatibility and content entered by its users, to the extent of its actions and applicable law. Connections to radios, third-party networks or external systems require the relevant authorisations and licences.

6 Nature of the evaluation and support

6.1 The trial is intended for controlled evaluation. It does not include commitments regarding continuous availability, coverage, latency, 24-hour service or a commercial SLA. Initial support must be requested at sales@coreptt.com for referral to the responsible team, subject to availability and the agreed scope.

6.2 The CUSTOMER must not rely exclusively on the trial environment for emergencies, rescue, personal safety or control of critical processes. It must maintain alternative communications and contingency arrangements throughout the evaluation. The platform does not replace public emergency services.

6.3 The PROVIDER will maintain reasonable security measures and may perform maintenance, corrections and adjustments, notifying foreseeable impacts where possible. A material interruption attributable to the platform may justify an extension if agreed in writing.

7 Data protection and privacy

7.1 The parties will comply with Brazilian Law No. 13.709/2018 (LGPD). For user, communication and location data processed on CUSTOMER instructions, the CUSTOMER will act as controller and the PROVIDER as processor. For commercial registration, contract management, fraud prevention and compliance with its own obligations, the PROVIDER may act as an independent controller according to the purposes actually adopted.

7.2 Processing may cover name, email, telephone, user or device identifier, access and usage records and, only when enabled, voice, video, messages and location. The purposes are to provide the trial, administer access, deliver support, protect the environment and assess its operation. Fictitious or anonymised information should be preferred where sufficient.

7.3 The CUSTOMER will determine the appropriate legal basis for its operations and inform data subjects in advance about monitoring, recording, location, purposes, access and retention periods. Acceptance of this agreement does not replace those steps or constitute blanket user consent. Sensitive data and data relating to children or adolescents are excluded from the trial unless a specific prior arrangement is made and legal requirements are met.

7.4 The PROVIDER will process data under lawful, documented instructions, restrict access to those who need it and adopt proportionate controls, including permission management, credential protection and relevant event records. It will not use communications content for advertising, sale to third parties or training AI models without a specific arrangement and an appropriate legal basis.

7.5 Hosting and support providers may be used only as necessary and subject to confidentiality and data protection obligations. The applicable provider list, processing location and any international transfer must be disclosed to the CUSTOMER before activation; where a transfer occurs, the relevant legal mechanisms and requirements must be met.

7.6 A party identifying an incident involving personal data will notify the other without undue delay, providing available information and updates for containment and assessment. The controller will assess and make notifications to the ANPD and data subjects where required, within statutory deadlines; the processor will provide the necessary cooperation. This allocation does not remove either party's own obligations.

7.7 Data subject requests, access and erasure rights and privacy matters may be sent to legal@coreptt.com. Each party is responsible for processing under its control and will cooperate with the other in responding to rights requests and lawful demands.

8 Data when the trial ends

8.1 The CUSTOMER must request or perform, by the end of the trial, exports of any data it wishes to retain, using available formats and features. Termination does not guarantee subsequent dashboard access. Export support and any migration must be arranged before expiry.

8.2 As a rule under this draft, in the absence of a service agreement or lawful preservation request, operational content will be deleted or anonymised within 30 calendar days after the trial ends. Residual backups will be purged within 90 days after the trial ends and will not be reused for operational purposes. These periods must be validated against the environment architecture before signature.

8.3 Records subject to statutory retention or necessary for the legitimate exercise of rights may be retained for the applicable period, with restricted access and a limited purpose. A subsequent service agreement does not guarantee recovery of content already deleted. Free access does not imply 90-day recording retention during the trial.

9 Confidentiality and intellectual property

9.1 Each party will protect non-public information received in connection with the trial, including credentials, settings, proposals, operational data and technical documentation. Access will be limited to persons necessary to perform this agreement who are subject to confidentiality duties. This obligation continues for 3 years after termination; trade secrets and personal data remain protected for as long as their nature and the law require.

9.2 Confidentiality does not cover information proven to be public, already lawfully known or obtained from a third party without breach of duty. Disclosure required by an authority will be limited to what is necessary and notified to the other party in advance where legally permitted.

9.3 The platform, its code, trademarks, interfaces and documentation belong to their respective owners. CUSTOMER data remains owned by the CUSTOMER or the relevant rights holders according to the nature

of the right. The trial does not authorise public use of a trademark, logo, testimonial or customer name as a commercial reference without specific authorisation.

10 Compliance integrity and governance

10.1 The parties will comply with applicable law, including anti-corruption rules and Brazilian Law No. 12.846/2013 where applicable. Offering or receiving improper benefits, fraud, unlawful favouritism and using the trial to circumvent purchasing processes, approval limits or internal controls are prohibited.

10.2 The CUSTOMER declares that the trial has been internally authorised. Each party will appoint a person responsible for decisions, access management and monitoring. Changes to scope, features, duration and service agreements will be documented and approved by persons with the authority to do so.

10.3 Trial governance will include permission control, revocation of unnecessary access, recording of approvals and assessment of results. Audits must be agreed in advance, be proportionate and protect third-party data, confidentiality and platform security; they do not grant unrestricted access to infrastructure or source code.

10.4 Suspected fraud, conflicts of interest, confidentiality breaches or irregularities may be reported to legal@coreptt.com, with handling restricted to those responsible for investigation and no retaliation for good-faith reports. This agreement establishes conduct obligations without claiming unsubstantiated certifications, audits or technical compliance.

11 Suspension termination and liability

11.1 The CUSTOMER may end the trial at any time by written notice, without a penalty or charge for the free licence. The PROVIDER may suspend or terminate access in the event of unlawful use, material breach, compromised security or an order from an authority. It will state the reason where permitted and offer an opportunity to remedy the issue where compatible with the risk; urgent measures may be immediate.

11.2 Each party is liable for damage it causes according to its conduct, causation and applicable law. Free access does not remove statutory duties of security, data protection and good faith. No automatic compensation is established, nor any exclusion for wilful misconduct, gross negligence or infringement of rights that cannot be excluded by contract.

11.3 Failures of internet, telecommunications operators, power and devices and force majeure events will be assessed according to their cause and each party's reasonable prevention and mitigation measures, without removing liability imposed by law.

12 Notices and final provisions

12.1 Sales and contracting: sales@coreptt.com. Registered telephone: (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. Notices to the CUSTOMER will use the contact details identified in this agreement, which must be kept up to date.

12.2 This agreement and the activation schedule form the evaluation agreement. External policies form part of it only if provided to the CUSTOMER before acceptance and identified by title, version and date. Future policies will not be incorporated automatically, nor will unilateral retroactive changes apply. Discrepancies will be resolved by written agreement between the parties, subject to mandatory rules.

12.3 Any forbearance does not constitute a waiver. Invalidity of one provision does not affect the others. After termination, confidentiality, data protection, intellectual property and liability obligations continue for the applicable periods.

12.4 The parties may sign physically or electronically using a method accepted by both, with records of authorship, integrity, version, date and time. The signatory declares that they have authority to represent the relevant party. Electronic signatures will comply with Article 10 of Brazilian Provisional Measure No. 2.200-2/2001 according to the method used and applicable requirements.

12.5 Brazilian law applies. The parties will seek an agreed resolution. The courts of the judicial district of Campinas/SP are selected because of their connection to the PROVIDER's registered office, subject to mandatory jurisdiction rules and applicable consumer protection provisions.

13 Acceptance and signatures

The parties declare that they have read and understood this agreement, validated the activation schedule and accepted the 7-day term, free access and termination without automatic conversion to a paid service.

Place and date: _____

PROVIDER COREPTT TECNOLOGIA LTDA

Representative: _____

Position: _____

Signature: _____

EVALUATING CUSTOMER [legal name]

Representative: _____

Position: _____

Signature: _____

WITNESSES Where used

1 Name: _____ CPF: _____

Signature: _____

2 Name: _____ CPF: _____

Signature: _____

Check before signature

Complete CUSTOMER and representative details; enter the start, end, limits and features; disclose hosting and providers; validate deletion and backup periods; and submit the draft for legal review before use.