



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