

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