Technical and Organizational Measures (TOM)

Effective: 26 Aug 2026 · Version 1.1 · Document set 2026-08_v1

Scope

This document describes the technical and organizational measures of EchoCall LLC under Art. 32 GDPR for the hub.echocall.de platform. It is Annex 2 to the Data Processing Agreement. The measures are continuously adapted to the state of the art without reducing the level of protection.

1. Physical and infrastructure security

- Operation exclusively in ISO 27001-certified data centres (IONOS, locations in Germany and France, in particular Frankfurt and Karlsruhe) with their physical security measures (access control, video surveillance, redundant power and network)
- EchoCall staff have no physical access to the data centres; physical security is evidenced by the infrastructure operator's certifications
- Encryption of data at rest at the storage level of the infrastructure (infrastructure operator IONOS)

2. Access control (authentication)

- Passwordless login via time-limited one-time codes (magic link/login code) or password login with bcrypt-hashed passwords
- Optional two-factor authentication (TOTP); 2FA secrets are stored encrypted with AES-256-GCM, backup codes hashed
- Session management via signed, HttpOnly cookies; live-chat agent sessions via signed JWT tokens
- Rate limiting and lockout mechanisms against brute-force attempts, IP-based registration throttling

3. Authorization control

- Role-based access control (customer, administrator, reseller) enforced server-side
- Granular per-area workspace permissions for team members; invitation and approval flow controlled by the account owner
- Strict tenant separation at the data level: every query is scoped to the owner context; resellers only see their own customers
- Public API only with HMAC-signed API keys, optionally with additional IP and domain whitelisting; full request logging
- Chat widget with domain whitelist against unauthorized embedding (fail-closed)

4. Transfer control

- Transport encryption TLS 1.3 (HTTPS enforced) for all connections between devices, the platform and sub-processors

- Credentials of customer systems (integrations) are stored server-side and never passed to language models; actions run through a platform webhook proxy
- SMTP credentials stored encrypted (AES-256-CBC); payment data is processed exclusively by the payment provider (PCI-DSS), EchoCall stores no card data

5. Input and traceability control

- Audit logs for security-relevant events (logins, failed attempts, administrative actions)
- Logging of document and invoice access
- Registration consents are stored with timestamp and version of the legal document set (Art. 7(1) GDPR)

6. Processor control

- Written contracts with all sub-processors under Art. 28(4) GDPR including Standard Contractual Clauses where third countries are involved
- Versioned contractual sub-processor list with a 30-day notice and objection procedure
- The entire speech processing chain (speech recognition, speech synthesis, LLM inference of the default profiles EchoCall-Voice/EchoCall-Smart) runs as EchoCall's own software on its own EU infrastructure, with no external speech or model provider in the conversation path; optional external model profiles are excluded from this assurance (Customer decision)

7. Availability control

- Redundant infrastructure of the data centre operator; availability target 99.9% (Enterprise 99.95%)
- Regular database backups; invoice documents are additionally backed up hourly to a separate backup server
- Error and availability monitoring (Sentry with EU ingest, transmission of personal data disabled), health checks for integrations
- Application-level rate limiting, baseline DDoS protection at the infrastructure level

8. Separation control

- Logical tenant separation of all customer data within the platform
- Whitelabel instances of the PartnerNet SaaS Titan plan are operated as separate instances
- Separation of production and development environments

9. Data minimization, retention and deletion

- Retention periods configurable per agent (1/7/30/90/365 days, custom up to 3650 days or unlimited); default for new agents: 30 days
- An automated daily cleanup removes transcripts, recording references and extracted conversation content after expiry from all stores of the platform (analytics database and agent runtime conversation store)
- Call recording can be disabled per agent; zero-PII mode prevents permanent storage of identifying conversation content
- GDPR deletion function in the Live Inbox with final deletion after a 30-day grace period

- Full account deletion removes all agents, knowledge bases, conversations, analytics content and files of the platform; invoice data subject to statutory retention is blocked and deleted after expiry

10. Incident management

- Documented process for detecting, assessing and handling security incidents with automated alerting
- Notification of affected customers without undue delay, at the latest within 48 hours of becoming aware of a breach affecting them
- Regular internal security reviews and code audits; findings are incorporated into the platform in documented form

Downloads

- TOM as PDF (English): https://echocall.de/documents/echocall-tom-en.pdf
- TOM als PDF (German): https://echocall.de/documents/echocall-tom-de.pdf

---