AUDICAP · TRUST CENTER

Technical and organisational measures under Art. 32 GDPR

As of 21 October 2026 · Version 1.1 · trust.audicap.app

Controller: IMA GmbH · Marketing & Consulting, Heinrich-Barth-Straße 17, 66115 Saarbrücken, Germany · Contact: privacy@audicap.app

Data protection officer: Anwaltskanzlei Stefan Wiesen, Mainzer Straße 161, 66121 Saarbrücken, Germany

This is a translation. The German version is authoritative.

Scope

These measures apply to the processing that IMA GmbH carries out itself for Audicap:

- the websites audicap.app and trust.audicap.app and email (server at Hetzner in Falkenstein),
- account, licence, subscription status, model downloads, updates and support via api.audicap.app (IMA GmbH's own server in Saarbrücken),
- building, signing and publishing the app.

Meeting content is out of scope. The app processes recordings, transcripts, summaries and speaker profiles exclusively on the user's device or, if the user sets this up, directly at the user's own cloud provider. They never reach IMA GmbH. The Trust Center section “App security” describes the app's protective functions.

1. Confidentiality (Art. 32(1)(b) GDPR)

1.1 Physical access control

- Website and mail server: data centre of Hetzner Online GmbH in Falkenstein. Hetzner is certified under DIN ISO/IEC 27001:2022 for the infrastructure and operation of its data centres (certification body SOCOTEC). Hetzner governs physical access under the data processing agreement.
- Licence server api.audicap.app: not a data centre but a locked server room on the premises of IMA GmbH in Saarbrücken. Only the management holds the key to the server room. The premises are secured by an alarm system and video surveillance.

1.2 System access control

- Only HTTP and HTTPS are reachable from outside, via a reverse proxy. HTTP redirects to HTTPS, and HSTS is set. The application itself and the management interfaces of the proxy and the virtualisation are not reachable from outside.
- The licence server's administration interface is reachable only from the IMA GmbH network and is rejected from outside. It has one administrator account, a password stored with bcrypt, protection against cross-site request forgery, at most ten login attempts per hour and IP address, a session cookie sent only over HTTPS and not readable by scripts, and sessions end after 24 hours. It has no two-factor login.
- Server administration via SSH; as root on the licence server only with a key. For administration, the licence server's network is reachable only on site or via a WireGuard VPN.
- Website server: administration via SSH with a key.
- Source code on GitHub: two-factor login for everyone with access.

1.3 Data access control

- The management and one further person have administrative access to the servers. Only the management holds the keys for signing the app.
- Access is granted only for the task at hand. When someone leaves, we revoke GitHub access, SSH keys and accounts on their last working day and change shared passwords.
- User account passwords are stored exclusively as bcrypt hashes (cost factor 12).
- Login links by email are valid for 15 minutes, pairing codes for the app for 2 minutes. Access tokens are valid for 15 minutes, refresh tokens for 30 days; refresh tokens, login links, password resets and program keys are stored only as hashes.
- Rate limiting: 100 requests per minute and IP address in general, 5 to 30 attempts per 15 minutes for login and password reset.
- The licence server refuses to start with default or too short secrets; login tokens, codes and state parameters are redacted in logs.

1.4 Separation control

- Website and licence server run on separate systems at separate locations.
- The licence service runs in its own container on its own virtual system (LXC) with its own database.
- Meeting content is separated by design: it is not stored on IMA GmbH systems.

1.5 Pseudonymisation and encryption (Art. 32(1)(a) GDPR)

- All connections to audicap.app, trust.audicap.app and api.audicap.app use HTTPS (TLS 1.3 for the licence server).
- Emails from audicap.app are protected with SPF, DKIM and DMARC.
- The licence server stores no payment data, only a Stripe customer reference.
- The copy of the backups at the separate location is stored encrypted. The on-site backup server and the licence server's own disks are not encrypted; they are located in the locked server room (1.1).
- Development and automated tests work without production data. We fetch a diagnostics package only for a specific support request, onto an encrypted work computer, and delete it after the analysis.
- The macOS build machine is encrypted with FileVault.

2. Integrity (Art. 32(1)(b) GDPR)

2.1 Transfer control

- Program updates are delivered only over HTTPS from api.audicap.app. The macOS app is signed with an Apple Developer ID and notarised by Apple; the Windows app is signed to IMA GmbH via Microsoft Azure Artifact Signing. The Windows updater installs only packages with this signature.
- The app checks speech models against pinned SHA-256 checksums before use.
- Published files are verified by SHA-256 on upload; every release ends with a check that the publicly delivered files match the approved build.

2.2 Input control

- Code changes go through the Git version control system; changes to the licence server are compared against the versioned state before they are applied.
- The licence server logs requests with time and IP address (retention see 5.).

3. Availability and resilience (Art. 32(1)(b) and (c) GDPR)

- Licence server: a daily backup during operation to an on-site backup server (a separate virtual machine on mirrored disks) and every night a copy to a physically separate location. Both locations keep 14 daily, 8 weekly, 12 monthly and 3 yearly versions. The backups are checked for readability weekly; a monitor reports when a backup is older than 26 hours.
- Recovery: at most the data since the last nightly backup is lost (up to 24 hours). The target for restoring the licence server is three working days. Restoring is tested annually in an isolated test environment, most recently on 19 October 2026 (service operational, database complete, checksums identical).
- Website server: daily backup, local and external. The website itself is also fully kept in version control.
- The licence service reports its health every 30 seconds; if it exits unexpectedly, Docker restarts it automatically.
- A monitor checks api.audicap.app every minute and sends a push notification on an outage and before the certificate expires.
- If the licence server fails, the app keeps working: a successfully checked licence stays valid for 14 days without a connection.
- The licence server and the virtualisation host install operating system security updates automatically; virtualisation software and containers are updated by hand.
- The server room has smoke detection and air conditioning. There is no uninterruptible power supply.

4. Regular review (Art. 32(1)(d) GDPR)

- These measures are reviewed annually and with every major change to the infrastructure.
- Everyone with access is bound to confidentiality.
- The data protection officer is Anwaltskanzlei Stefan Wiesen, Saarbrücken.
- The management assesses personal data breaches without delay together with the data protection officer. We report notifiable cases to the Unabhängiges Datenschutzzentrum Saarland within 72 hours and notify the data subjects where the risk is high (Art. 33 and 34 GDPR). Every incident is documented.
- Vulnerabilities are received at security@audicap.app; the reporting channel and deadlines are set out in the public policy at audicap.app/en/security.html, machine-readable under RFC 9116.
- Subprocessors are listed in the Trust Center; we announce changes in advance by email.

5. Data protection by design and deletion (Art. 25 GDPR)

- Meeting content stays on the device; new installations use local models by default.
- Crash reports, access for AI assistants and phone transfer are off by default.
- A diagnostics package is attached to a support request only if the user explicitly ticks the box; it is deleted after 90 days.
- The licence server deletes expired tokens and codes every six hours.
- Application logs are deleted after 30 days, reverse proxy access logs after five weeks at most, its error logs after eleven weeks at most. Website logs are rotated daily and deleted after 30 days at most (currently after ten days).
- Download logs (IP address, browser or program identifier) are limited to 30 days; automatic deletion has been commissioned, until then they are deleted by hand.

- Support requests are deleted on request unless a retention obligation applies. Accounts can be deleted in the app (from version 0.13.0) or on request; running subscriptions are cancelled in the process.