aimachine.io
Privacy/Datenschutz

The AI Machine UG (haftungsbeschraenkt)
66333 Voelklingen, Germany
team@aimachine.io

2026-11-17

This document applies to aimachine.io, magiccap.aimachine.io, infinity.aimachine.io, armoredfile.aimachine.io and ephcall.aimachine.io. The current HTML version is available at https://aimachine.io/privacy.html. The shared legal notice and privacy notice are available at https://aimachine.io/legal.html and https://aimachine.io/privacy.html.

1 Controller and scope

The controller is The AI Machine UG (haftungsbeschraenkt) (hereinafter "The AI Machine"), 66333 Voelklingen, Germany, represented by Managing Director Dr. Yves J. Hilpisch. Contact The AI Machine about privacy and your rights at team@aimachine.io. Further company details are at https://aimachine.io/legal.html

This notice covers aimachine.io, its documentation and integrity tools, and every app or digital service that The AI Machine makes available, including apps distributed through TestFlight or the App Store. It applies to MagicCap, Infinity, ArmoredFile and EphCall, and to future apps to the extent they process personal data as described here. No account is required for the current public browser apps. Restricted administration and statistics login pages are separate from those apps. An app-specific privacy notice or in-app disclosure will explain additional processing or product-specific details and supplements this notice; this notice does not imply that an unreleased app already has the same data practices as the current browser apps.

2 Website delivery and server logs

When you open a page or download an asset, The AI Machine's hosting infrastructure processes your IP address and technical request data to deliver it. The web server records access and error logs. Access logs include the network address, request time, requested URL including any query string, response status, response size, referring URL, browser user-agent string and requested hostname. An authenticated username may be logged where HTTP authentication is used.

The AI Machine uses technical request data to operate the websites, diagnose faults and investigate misuse. The legal basis is Article 6(1)(f) GDPR: The AI Machine's legitimate interests in reliable delivery and protection of the service. The hosting provider and authorised administrators can process these technical records. No chat text, file content or microphone audio is deliberately sent to the web server by the communication apps.

The current server configuration rotates non-empty logs daily and retains 365 rotated files per log, plus the current file. Empty logs are not rotated, so this is a rotation-count limit rather than a guaranteed deletion deadline of 365 days. This retention applies to server records, independently of the much shorter application sessions.

3 Statistics derived from server logs

The AI Machine also derives internal usage statistics from the server access logs. The analysis uses IP addresses to count distinct daily visitors and browser user-agent strings to distinguish likely automated traffic. The statistics database stores daily counts, requested page paths without query strings and referring domains; it does not store the individual visitor IP addresses used for those counts.

The purpose is to understand service usage and automated traffic. The AI Machine relies on Article 6(1)(f) GDPR and its legitimate interest in operating and evaluating the websites. This analysis runs on the server without a browser analytics beacon or advertising cookie. The statistics database currently has no scheduled age-based deletion. Page paths and referring domains can themselves contain identifying information, so these statistics should not be assumed to be anonymous.

4 Peer connections and external infrastructure

When you enter an app and establish a connection, the app uses PeerJS cloud signaling and Google's STUN services. These external services receive connection metadata such as network addresses, peer identifiers and connection timing as needed for their respective functions. The other participant can also learn your network address. Encryption protects communication content but does not conceal these connection details.

The AI Machine processes connection identifiers and session state to provide the communication you request, on the basis of Article 6(1)(b) GDPR. Technical security and abuse prevention also serve The AI Machine's legitimate interests under Article 6(1)(f) GDPR. The current apps explicitly configure Google STUN servers and do not configure a TURN relay. Client-side libraries are delivered with the apps rather than loaded from an external executable CDN.

PeerJS cloud and Google operate infrastructure outside The AI Machine's control. Their retention and processing arrangements are separate from The AI Machine's local session handling and web-server log rotation. Information about their processing is available from https://peerjs.com and https://policies.google.com/privacy

External service processing and remote access can involve countries outside the EEA, including the United States. The AI Machine does not promise that connection metadata remains within the EEA. Contact The AI Machine at team@aimachine.io for information about recipients, processing locations and any applicable transfer safeguards, including how to obtain a copy. This notice does not treat encryption or a request to connect as consent to an otherwise unprotected international transfer.

5 Browser storage, permissions and session lifetime

MagicCap stores a peer identifier and display handle in sessionStorage. Infinity stores a peer identifier and display handle there, and EphCall stores a peer identifier. These entries help keep your chosen identifier available within the browser tab. They normally last until the tab is closed; browser session restoration can preserve them. Disconnecting a connection does not necessarily clear every stored identifier. ArmoredFile holds its transfer state in browser memory.

Session state, shared secrets and cryptographic keys are processed in your browser to establish and protect the requested communication. They are not deliberately saved as server-side content by the apps. Clearing application state is not a guarantee of secure erasure from device memory, operating-system facilities, backups or the other participant's device.

The public pages do not use advertising cookies or browser analytics beacons. Storage and access strictly necessary to provide a service you expressly request are treated under Section 25(2) TDDDG; this exemption does not remove GDPR obligations. The public apps do not require acceptance of tracking to work. Browser microphone permission is requested by EphCall for audio calls; a browser permission prompt does not replace this notice.

6 What differs between the apps

- MagicCap: encrypted messages are displayed temporarily, normally for about 60 seconds. Disappearing from the app does not prevent another participant from copying, photographing or otherwise recording them.
- Infinity: session-history retention in memory is optional and defaults off. Retained history is bounded to 1 MiB and 10,000 events. Exported encrypted and signed logs are downloaded files under the user's control and can remain on devices indefinitely. The app also processes imported log files locally for inspection and verification. A signature does not by itself establish a person's legal identity or recording consent.
- ArmoredFile: selected files, file metadata, encrypted chunks and keys are processed in browser memory for transfer. Expiry or reset of the transfer session does not delete the sender's original file or a recipient's downloaded copy. The current receiver has a 64 MiB in-memory file limit.
- EphCall: microphone audio is processed for the requested call. Strict insertable-stream media E2EE is enabled by default and blocks unsupported calls. Transport-only mode requires an explicit opt-out of strict mode. The app does not provide server-side voice recording, but the other participant or device software may record audio.

7 Messages to The AI Machine and other recipients

If you email The AI Machine, The AI Machine processes your email address, message and any supplied attachments to handle your request. The legal basis is Article 6(1)(b) GDPR for contractual or pre-contractual requests and Article 6(1)(f) GDPR for other correspondence, reflecting The AI Machine's interest in responding. The AI Machine's email service provider and authorised staff can receive that correspondence. The AI Machine retains correspondence for the time needed to resolve the request and any applicable legal retention or claim-preservation period.

Service providers involved in hosting and email, the external connection services described above, Apple when you use an app distributed through TestFlight, your chosen communication participants and authorities where legally required are possible recipients. The AI Machine does not sell personal data. You control which participant receives content; recipients may retain or redistribute it independently.

8 iPhone apps and TestFlight

When an app provided by The AI Machine is distributed as a beta through Apple's TestFlight service, Apple and The AI Machine as the app provider receive beta crash logs and usage data under Apple's TestFlight terms. These data can include device and software details, performance information, network information and how the beta app is used. Apple describes this collection as automatic for TestFlight beta apps. Apple processes information for its own TestFlight purposes under its privacy terms; The AI Machine uses data made available through TestFlight to evaluate and improve its apps and may contact testers about their use of a beta app.

TestFlight also lets testers send feedback, including written comments and screenshots, to Apple and/or The AI Machine. If you choose to submit feedback, it may contain personal information or content visible in a screenshot. Please review it before sending and do not include information about other people unless you are entitled to share it. An app's TestFlight details and any app-specific privacy notice will describe the data for that beta. Apple's processing is governed by Apple's own notices and terms, including https://www.apple.com/legal/internet-services/itunes/testflight/ and https://www.apple.com/legal/privacy/data/en/test-flight/.

9 Captain Memo (iOS beta)

Captain Memo is a voice-first personal organizer for iPhone, distributed as an invited TestFlight beta. Organizational dataincluding lists, tasks, notes, managed objects, service plans, reminders and settingsis created and stored locally on your device using Apple's SwiftData framework. The app requires no account, operates no backend of The AI Machine, and contains no analytics or tracking. The app does not transmit this organizational data or speech audio to a backend operated by The AI Machine; information you choose to include in TestFlight feedback is handled as described below.

Optional functions use Apple frameworks. Speech recognition may process audio on device or through Apple's services, depending on your iOS version and device settings; Apple's processing is governed by your Apple ID settings and Apple's privacy terms. Apple Intelligence interpretation is off by default, runs strictly on device and is enabled only if you opt in. Camera import of handwritten lists uses Apple's on-device Live Text processing.

For Captain Memo's TestFlight beta, TestFlight automatically collects crash diagnostics and usage metadata and makes them available to Apple and The AI Machine through App Store Connect. You may also choose to submit feedback, including screenshots, through TestFlight; review it for personal or organizational information before sending. The general TestFlight information above applies. Beta software may contain errors; do not keep irreplaceable information only in the beta. Backups you export are ordinary files under your control. Optional local command history is off by default and can be deleted at any time. Removing the app deletes its local store.

10 Your rights and complaints

Subject to the applicable conditions, you can request access, correction, erasure, restriction and data portability. You can object to processing based on legitimate interests on grounds relating to your particular situation. If processing is based on consent, you can withdraw it for the future without affecting earlier lawful processing. Contact The AI Machine at team@aimachine.io to exercise your rights.

The AI Machine may be unable to associate an ephemeral session with you after it ends, and The AI Machine does not collect additional identifying information just to identify past session participants. The AI Machine will explain any limits on fulfilling a request and may ask for proportionate identity verification. The AI Machine cannot erase copies independently held by other participants.

You may complain to a data protection supervisory authority, including the Unabhaengiges Datenschutzzentrum Saarland: https://www.datenschutz.saarland.de or the authority where you live or work.

11 Required information and automated decisions

You do not have to create an account or provide your real name. Network addresses are technically necessary to deliver pages and establish connections. A peer identifier and shared secret are needed for the requested authenticated sessions, and EphCall needs microphone access for a call. Without the relevant information or permission, those features cannot operate. Avoid putting personal data or secrets in URLs or handles.

The AI Machine does not use the public suite to make decisions producing legal or similarly significant effects about you solely by automated processing. The AI Machine updates this notice when processing changes; its effective date is stated above.