

Support for the Data Protection Impact Assessment (DPIA)

LocalTranscript · Documentation for IT and data protection

Status: version 0.6.65, September 2026

This document supports the data protection officers of your organisation in assessing LocalTranscript as part of a data protection impact assessment under Art. 35 GDPR.

Classification: No Agreement for Processing on Behalf of a Controller for the Local Product

Using LocalTranscript in its default local configuration does not create **processing on behalf of a controller within the meaning of Art. 28 GDPR** between your organisation and Jenzer Innovations. Reason: we do not process any data belonging to your organisation. Recording, transcription, speaker recognition, voiceprint matching, and AI summarization run entirely on your organisation's workstation; there is no cloud service, no user account, and no transmission path for meeting content to us. Your organisation remains the sole controller within the meaning of Art. 4 No. 7 GDPR for the data generated with the application; we do not act as a processor, because we do not, in fact, process anything that would be accessible to us.

An agreement for processing on behalf of a controller becomes relevant only once your organisation activates **optional, explicitly opt-in** connected services (e.g. a cloud provider for transcription/AI actions, the mobile companion using our relay path outside the local network, or support with data access). These are disabled in the default configuration and can be disabled organisation-wide via administrative policy (`policy.json`) (see our document "Administrative policy").

The following template is intended to be filled in and adapted by your organisation.

1. Description of the Processing

Purposes of the processing: Recording, transcription, and documentation of meetings/conversations in an official context; automatic speaker recognition to attribute conversational contributions; optional AI-assisted summarization and keyword extraction from the transcript; storage and searchability of past meetings.

Categories of data subjects: Employees of your organisation who take part in recorded meetings; where applicable, external interlocutors (citizens, contractual partners, other public authorities or companies), to the extent their conversations are recorded.

Categories of personal data:

- Spoken language as an audio recording and its transcription (transcript)
- Name/designation of the speaking person, if stated in the conversation or attributed via speaker recognition

- Substantive information from the course of the conversation (topic, notes, where applicable special categories of personal data, if mentioned in the conversation itself – e.g. health data in a counselling conversation)
- **Optional, Art. 9 GDPR:** Voiceprints (biometric characteristics for automatically recognizing a speaker again across multiple meetings) – only if the feature is activated and consent has been recorded for the respective contact. The feature can be disabled organisation-wide.
- Metadata (timestamp, device name of the recording location, duration)

Processing location: Exclusively the respective workstation within your organisation. No server, no cloud processing in the default configuration. Optional cloud providers (if deliberately activated by your organisation) are named in the network disclosure.

Storage duration: See our deletion concept – default retention is unlimited until actively deleted by the user; optional retention periods per category (meetings, audio, dictation snippets, audit logs) can be set in the application.

2. Legal Bases

[to be determined by your organisation] – depending on the specific purpose of use and the applicable state law. The following typically come into consideration:

- Art. 6(1)(e) GDPR (performance of a task carried out in the public interest or in the exercise of official authority) in conjunction with the respective sector-specific legal basis, if the recording is necessary for the performance of the task
- Art. 6(1)(c) GDPR, if a legal obligation to keep records exists
- § 26 BDSG (German Federal Data Protection Act) or the corresponding state-law provision, insofar as employee data is affected, where applicable in conjunction with a works/service agreement (check staff council co-determination)
- Art. 6(1)(a) GDPR (consent) for participants whose recording is not already covered by one of the aforementioned bases – the application requires a consent confirmation before every recording and logs it completely
- **For voiceprints (Art. 9 GDPR):** typically Art. 9(2)(a) GDPR (explicit consent), since other exemptions are rarely applicable here; the application records this consent per contact and refuses voiceprint capture without it

3. Necessity and Proportionality

Recording and transcription serve to document meetings and make them traceable, and relieve employees of manual minute-taking. Proportionality is supported by several application-level design choices:

- Processing exclusively local, no disclosure to third parties in the default configuration
- Voiceprints (the most privacy-intrusive data category) are a separately activatable feature with its own consent recorded per contact, and can be fully disabled organisation-wide
- Data subjects can object at any time or decline the recording of an individual meeting (consent prompt before recording begins)

- Deletion is possible granularly (individual meeting, individual audio track, individual voiceprint) rather than only completely
- Retention periods are configurable

A milder, equally effective alternative (e.g. purely manual minute-taking) generally does not achieve the same degree of completeness and traceability; the final balancing assessment is the responsibility of your organisation.

4. Risks for Data Subjects

Risk	Likelihood	Severity	Measure	Residual Risk
Unauthorized access to the workstation (e.g. unlocked screen)	Medium	High	Access protection via Windows/macOS user account; recommendation: screen lock, multi-factor authentication at sign-in (organisational measure of your organisation)	Low to medium, depending on your organisation's implementation of sign-in security
Loss or theft of the device	Low	High	Voiceprints are already encrypted; disk encryption (BitLocker/FileVault) is recommended for meeting data overall – additional application-level encryption at rest is planned but not yet shipped	Medium, until disk encryption is implemented by your organisation or application-level encryption becomes available
Recording without the knowledge of the conversation participants	Low	High	Mandatory consent confirmation before every recording start, logged completely (consent log)	Low
Voiceprints: biometric re-recognition without the data subject's knowledge	Low	High	Feature has no automatic capture by default; requires consent recorded per contact; can be fully disabled organisation-wide	Low
Exporting a transcript to a cloud-synced folder (e.g. OneDrive) without being aware of it	Medium	Medium	The application detects cloud-synced target folders during Markdown export and warns about it	Low to medium, depending on user behaviour after the warning
Dictated text reaches another, unintended application or its history via the clipboard	Low	Medium	Dictation excludes inclusion in clipboard history and cloud clipboard, and restores the previous clipboard content afterward	Low
Terminal server/multi-user operation: another signed-in account eavesdrops via a local interface port	Low	High	Local interfaces (MCP integration, local AI server) are disabled by default, reachable only via the local network address <code>127.0.0.1</code> , and additionally protected by an access token newly generated at every	Low

5. TOM List (Technical and Organisational Measures)

Category	Measure of the Product	Measure of Your Organisation
Physical Access Control	–	Physical access security to the office premises/workstations
System Access Control	No separate user account for the application; access exclusively via the operating system user account	Windows/macOS sign-in with multi-factor authentication (e.g. Windows Hello for Business, FIDO2), screen lock
Data Access Control	Secrets and voiceprints stored encrypted in the user profile; local interfaces token-protected and restricted to 127.0.0.1	Access rights at the operating system level, group policies
Transfer Control	A single network chokepoint with logging; Hard Offline Mode; cloud providers off by default and disable-able via policy; end-to-end encryption for the optional mobile companion	Roll out the administrative policy (policy.json) to disable cloud usage organisation-wide
Input Control	Network audit log, MCP audit log, complete consent log, each exportable	Regular review/archiving of the exported logs according to its own requirements
Availability Control	Fully local, offline-capable processing with no dependency on our availability	Backup of the local data folder is the responsibility of your organisation
Separation Control	Data is kept separate per operating system user account; local interfaces are additionally bound to a token or account	Separate user accounts per employee, no shared accounts
Contract Control (Art. 28 GDPR)	Not applicable for the default local configuration (no processor, see section "Classification")	When optional cloud providers are activated: a separate agreement for processing on behalf of a controller with the respective provider is required

6. Rights of Data Subjects

Right of access (Art. 15 GDPR): Meetings in which a specific person participated can be found in the library view via full-text/contact search by name, time period, or keyword. Your organisation, as the controller, can export the corresponding transcript and make it available to the person requesting access. The consent log additionally documents when and by what means consent to the recording was given.

Erasure (Art. 17 GDPR): An individual meeting, including audio, transcript, and derived data, can be deleted specifically (see our deletion concept); likewise for an individual voiceprint. "Delete All Data" is available for a complete deletion of all locally stored data. Since processing takes place exclusively locally, your organisation handles access and erasure requests itself, without any request to us being necessary – we hold no copy of the data.

7. Record of Processing Activities (Art. 30 GDPR) (Sample Entry to Insert)

Name of the processing activity: Recording and transcription of official meetings using LocalTranscript

Controller: [Name of your organisation, address]

Data protection contact: [data protection officer of your organisation]

Purposes of the processing: Documentation of meetings; automatic transcription; optional speaker recognition; optional AI-assisted summarization

Legal basis: [to be determined by your organisation, see Section 2 of this document]

Categories of data subjects: Employees; where applicable, external interlocutors

Categories of personal data: Audio recording, transcript, speaker attribution/name, conversation content; optionally voiceprints (Art. 9 GDPR)

Recipients: None – processing exclusively local on the workstation; no processor in the default configuration

Transfer to third countries: None in the default configuration; arises only upon deliberate activation of an optional cloud provider not established in the EU/EEA

Retention periods: See deletion concept (attachment), default retention unlimited until actively deleted; optional retention periods configurable

Technical and organisational measures: See security concept and TOM list (attachments)

8. Assessment Result

Date of assessment: _____

Result:

- ☐ Risk to the rights and freedoms of data subjects is acceptable; the measures presented are sufficient
- ☐ Further measures required (see remarks)
- ☐ Prior consultation of the supervisory authority required (Art. 36 GDPR)

Remarks:

Data protection officer: _____ Date: _____

Signature: _____