**Data Protection Impact Assessment (DPIA) – Architectural Justification for On-Device Transcription**

1. System Description & Data Flow (Verarbeitungstätigkeit)
Unlike traditional SaaS (Software-as-a-Service) transcription providers, the proposed solution (Geode) operates under a "Local-First" architecture.

Processing Location: All audio processing and text generation occur exclusively on the end-user's local hardware (Mac).

Data Transfer: No audio data, metadata, or generated text transcripts are transmitted to external servers, cloud providers, or third-party subprocessors for processing.

Network Dependency: The core transcription engine functions offline. Network activity is limited to license validation or software updates, not data processing.

2. Assessment of International Data Transfer Risks (Drittlandtransfer)
Schrems II Relevance: N/A.

Justification: Since no personal data is transmitted to cloud infrastructure (whether in the EU or third countries like the USA), the legal uncertainties regarding cross-border data transfers (Art. 44 et seq. GDPR) are architecturally eliminated.

Supplementary Measures: No supplementary measures (encryption in transit, SCCs, TIAs) are required for the transcription process itself, as the data never leaves the controller's (the organization's) physical possession.

3. Compliance with GDPR Core Principles (Art. 5)
Integrity and Confidentiality (Art. 5(1)(f)):

Risk: In cloud environments, confidentiality depends on the vendor's security posture and subprocessor chain.

Mitigation: With on-device processing, confidentiality is defined solely by the organization's existing endpoint security (disk encryption, device access controls). The attack surface is reduced from "Public Cloud" to "Single Device."

Data Minimization (Art. 5(1)(c)):
The system does not contribute to "Data Gravity" in vendor clouds. No copies of meetings are stored on external servers "just in case." Data exists only where the user explicitly saves it.

Privacy by Design & Default (Art. 25):

The application adheres to the strictest definition of Privacy by Design: the technical impossibility of vendor access. The vendor cannot access the data even if compelled by law enforcement, as they do not possess the keys or the data.

4. Risk Assessment Overview

| Risk Category | Cloud-Based Transcription | On-Device Transcription (Geode) |
|---|---|---|
| Vendor Data Access | Possible (Support/Ops/Legal) | Impossible (Technical Constraint) |
| Subprocessor Breach | High Dependency Risk | No Subprocessors involved |
| US Cloud Act Exposure | Potential Risk | Eliminated (Data remains local) |
| Employee Surveillance | Usage logs often centralized | Local only / User Controlled |

5. Conclusion for the Data Protection Officer

The implementation of on-device transcription represents a significant reduction in compliance risk compared to cloud-based alternatives.

By keeping the processing of potentially sensitive conversations (which may include Article 9 special categories of data) strictly within the organization's hardware perimeter, we bypass the complexities of Data Processing Agreements (AV-Vertrag) for this specific workflow.

Recommendation:

From a data sovereignty perspective, this architecture satisfies the requirements of Datensparsamkeit (data minimization) and eliminates the need for a Transfer Impact Assessment (TIA) for meeting data.