Bericht zur DSGVO-Konformität der Aliru GmbH

Einleitung

Die Aliru GmbH bietet eine KI-gestützte Softwarelösung zur automatisierten Meeting-Dokumentation an. Dabei werden Audio- und Videoaufnahmen verarbeitet, um Transkripte zu erstellen und Meetings effizient zu dokumentieren. In diesem Bericht wird dargelegt, warum die Verarbeitung dieser Daten DSGVO-konform erfolgt. Die wichtigsten Aspekte der DSGVO werden erläutert und auf die implementierten Maßnahmen eingegangen.

1. Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)

Die Verarbeitung von Audio- und Videoaufnahmen durch die Aliru GmbH erfolgt ausschließlich im Auftrag der Kunden. Die Kunden sind für die Einhaltung der rechtlichen Voraussetzungen verantwortlich und müssen die Einwilligung der Teilnehmer einholen. Sally, die KI-gestützte Meeting-Dokumentation, informiert alle Anwesenden bei Betreten des Meetings über ihre Anwesenheit und stellt einen Link mit Datenschutzinformationen bereit.

Da die Aliru GmbH als Auftragsverarbeiter im Sinne des Art. 28 DSGVO agiert, erfolgt die Verarbeitung stets auf Weisung des Kunden, der die Rolle des Verantwortlichen übernimmt.

2. Transparenz und Informationspflicht (Art. 12-14 DSGVO)

Die Aliru GmbH stellt sicher, dass betroffene Personen transparent über die Datenverarbeitung informiert werden. Dies geschieht durch:

- Die automatische Information aller Meeting-Teilnehmer durch Sally
- Bereitstellung einer Datenschutzerklärung über einen Link im Meeting-Chat
- Nutzer können der Verarbeitung durch Deaktivierung der Software im Meeting widersprechen.

3. Verarbeitung personenbezogener Daten

Die Software verarbeitet:

- Gesprochene Sprache (Transkripte)
- Metadaten (Datum, Uhrzeit, Meeting-ID, Teilnehmerliste – falls bereitgestellt)
- Videoaufnahmen (wenn aktiviert, zur Unterstützung der Transkription)

Aliru selbst hat keinen Zugriff auf die Inhalte der Meetings oder Videoaufzeichnungen. Die Daten werden verschlüsselt gespeichert und stehen ausschließlich dem Kunden zur Verfügung.

4. Auftragsverarbeitung und Verantwortung (Art. 28 DSGVO)

Die Aliru GmbH agiert als Auftragsverarbeiter und verarbeitet personenbezogene Daten ausschließlich auf Weisung des Auftraggebers. Dies ist durch den abgeschlossenen Auftragsverarbeitungsvertrag (AVV) geregelt, welcher folgende Aspekte abdeckt:

- Verarbeitung erfolgt ausschließlich innerhalb der EU (vorzugsweise Deutschland)
- Kunden behalten die Kontrolle über ihre Daten und können diese jederzeit verwalten oder löschen (es erfolgen keine Back-Ups oder Speicherung der Daten seitens der Aliru GmbH)
- Subdienstleister sind in einer Anlage des AVV gelistet und unterliegen denselben Datenschutzauflagen

5. Maßnahmen zur Datensicherheit

Die Software erfüllt die Anforderungen des Art. 32 DSGVO zur Sicherheit der Verarbeitung durch technische und organisatorische Maßnahmen (TOMs), darunter:

- Zugangskontrollen: Hosting in EU-Rechenzentren mit ISO 27001-Zertifizierung.
- Zugriffskontrollen: Authentifizierte und autorisierte Nutzung durch Kundenkonten.
- Verschlüsselung: AES-256 für gespeicherte Daten, TLS/SSL für Übertragungen.
- Protokollierung: Lückenlose Nachvollziehbarkeit von Zugriffen und Änderungen.
- Löschkonzept: Daten werden nach den vom Kunden definierten Fristen automatisch gelöscht.

6. Speicherdauer und Löschung (Art. 5 Abs. 1 lit. e DSGVO)

Die Aliru GmbH speichert keine Daten über die vom Kunden festgelegte Dauer hinaus. Kunden können Transkripte und Videoaufnahmen selbstständig verwalten und löschen. Es gibt keine automatische Löschung durch Aliru GmbH, sondern volle Kontrolle für die Kunden.

7. Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO)

Der AVV enthält klare Regelungen zur Meldung von Datenschutzverletzungen. Dazu gehört:

- Verpflichtung des Auftragsverarbeiters zur Meldung innerhalb von 24 Stunden nach Kenntniserlangung
- Detaillierte Anforderungen an die Meldung (Beschreibung, betroffene Daten, Ursachen, ergriffene Maßnahmen)
- Unterstützung des Auftraggebers bei der Meldung an die Aufsichtsbehörde

Fazit

Die Aliru GmbH hat umfangreiche Maßnahmen implementiert, um eine DSGVO-konforme Verarbeitung sicherzustellen. Insbesondere durch klare vertragliche Regelungen, hohe Sicherheitsstandards und die Verpflichtung zur Transparenz wird die Einhaltung der DSGVO sichergestellt. Kunden haben volle Kontrolle über ihre Daten, und die Verarbeitung erfolgt ausschließlich in der EU. Daher wird die Verarbeitung als DSGVO-konform eingestuft.

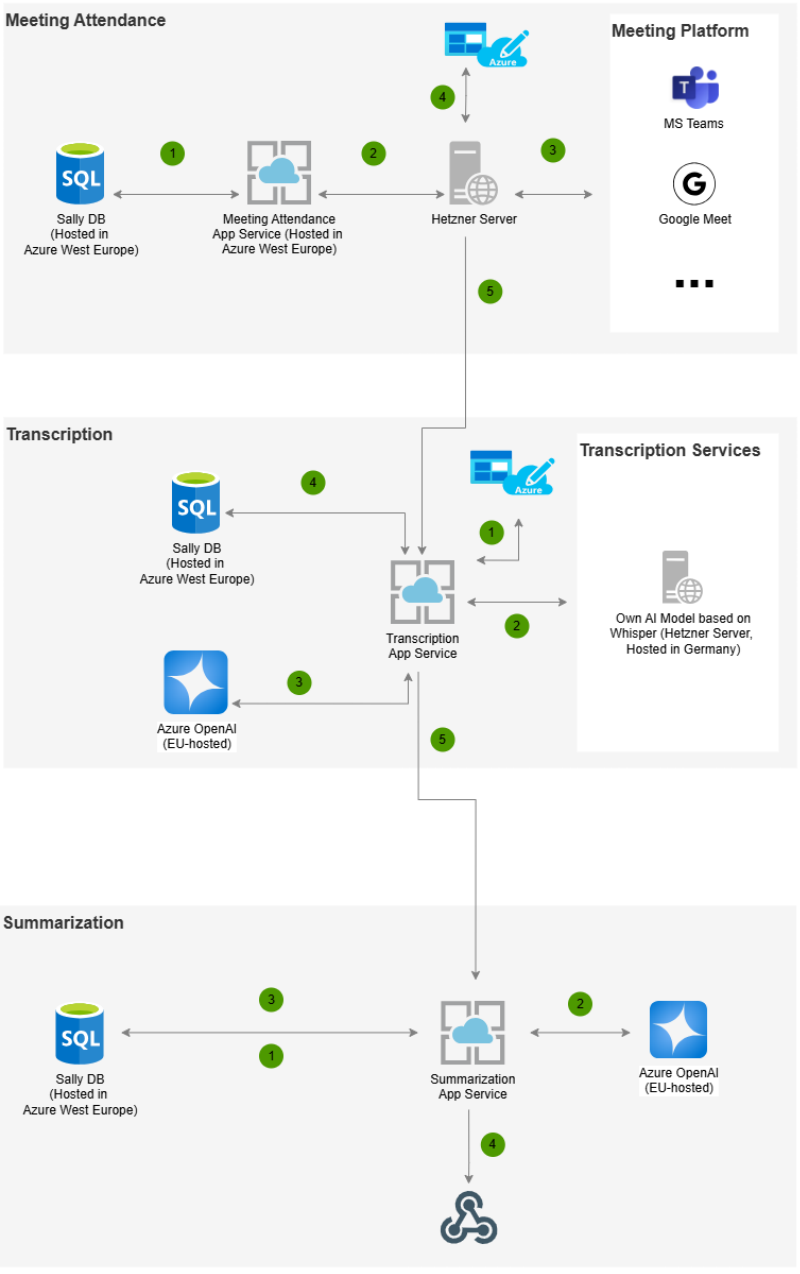
Zusätzliche Anmerkung

Die Aliru GmbH unterstützt Transparenz und vertrauensvolle Partnerschaften. Wir sind daher gerne bereit, auf Wunsch des Kunden an einem strukturierten Due-Diligence-Prozess teilzunehmen und eine entsprechende Vereinbarung zu unterzeichnen. Ziel ist es, eine umfassende Prüfung unserer Datenschutz- und Sicherheitsmaßnahmen zu ermöglichen und den Kunden in seiner Compliance- und Risikobewertung bestmöglich zu unterstützen.

_____

Aliru GmbH
Julian Kissel
CEO

SALLY



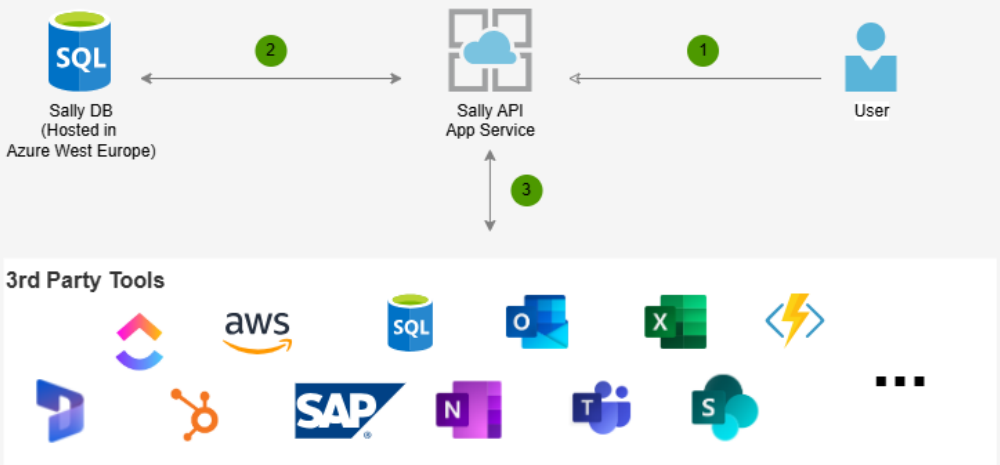
1. The Meeting Attendance Service uses the Sally DB data to check whether attendance at a meeting is expected. Both systems are hosted in Azure in the 'West Europe' data centre.
2. If a meeting has been found that Sally should attend, a new Hetzner node is started in our Kubernetes cluster and the meeting url is passed to the service. The service itself was programmed 100% in-house and Hetzner is only the infrastructure provider. The Hetzner servers used are located within the EU.
3. The new Hetzner node within the Kubernetes cluster emulates a meeting participant, starts the meeting participation and starts the meeting recording in the form of a video or audio file (depending on the setting). This continues until the meeting is finished, Sally is removed from the meeting or the term 'Opt out' is written in the chat. In the case of 'Opt out', the process stops at this point.
4. As soon as the meeting has ended or Sally has been removed from the meeting, the Hetzner Kubernetes node saves the data in an Azure Blob Storage.
5. The Hetzner Kubernetes node makes an HTTPS request to start the transcription service.

1. Based on the HTTPS request, which starts the transcription service, the audio file is loaded from the Azure Blob Storage. Like all other communication, the transfer takes place via encrypted communication.
2. Transcription is normally carried out via our in-house transcription service, which runs on a server with a graphics card (GeForce 4090 24GB or comparable) with our own trained AI model based on the Whisper model. We train only on our internal data: No customer data is included!
3. Once the transcription is complete, we use various AI prompts based on Azure Open AI (model: GPT-5.2, GPT-5-Mini or newer model) to further optimise the transcription. The hosted resources are located within the EU and are GDPR compliant. It is ensured that the data is NOT used for further training. Personal data is exchanged with placeholders BEFORE use and used afterwards.
4. The transcript is stored in the Sally DB (data centre: West Europe). The connection between the systems is encrypted for the transport.
5. Once the transcript is ready, the summary service is started via an encrypted HTTPS connection.

1. Based on the HTTPS request, the Summarisation Service, which is hosted within the EU (Azure data centre: West Europe), loads from the Sally DB via encrypted connection the information from the transcription and also all additional data known for the appointment (subject, description, participant, start time, end time, location).
2. The Summarisation Service then applies several consecutive prompts in Azure Open AI (model: GPT-4o, o3-mini or a newer model). The hosted resources are located within the EU and are GDPR compliant. It is ensured that the data is NOT used for further training. Personal data is exchanged with placeholders BEFORE use and used afterwards.
3. The resulting data or information is simply written back to the database. Only an encrypted connection is used for this. The data itself is also stored in the database in encrypted form.
4. After the summary & transcription are fully saved, the system calls user-configured webhooks (HTTPS, Zapier, Power Automate, ...). This is an optional step as it is configured by the user. If nothing is configured, this step is skipped.

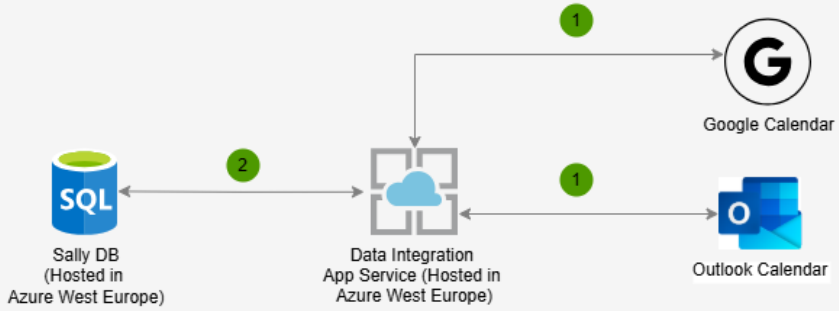
SALLY

Integration 3rd Party - Synchronization



1. As part of the native integration of 3rd party tools, the user has the option of transferring data to third party systems such as Asana, Trello, OneNote, SAP, Hubspot, Dynamics, etc. via a keyed connection. The use of this service is the sole responsibility of the user and is optional and manual.
2. The Sally API loads the data to be transferred from the Sally DB (hosted in Azure in the West Europe data centre) via an encrypted connection.
3. The data is transferred to the third-party system exclusively via an encrypted connection. The prerequisite for the transfer is the disclosure of the login information for the third-party system by the user. We use the so-called OAuth procedure for the login process and store the resulting token (as well as the refresh token) within the Sally DB.

Calendar - Appointmentsynchronisation



1. With the help of the Google Calendar API and the Outlook API (Microsoft Graph API), the data of the appointments (subject, description, start/end time, location, participant ICalID) are loaded. This task is done within an Azure App Service located in West Europe (Netherlands).
2. The loaded data is stored in an Azure SQL Database located in West Europe (Netherlands).