Report on GDPR Compliance of Aliru GmbH

Introduction

Aliru GmbH offers an AI-powered software solution for automated meeting documentation. This involves the processing of audio and video recordings to generate transcripts and efficiently document meetings. This report outlines the reasons why such data processing is conducted in compliance with the General Data Protection Regulation (GDPR). The key provisions of the GDPR are explained, and the implemented measures are presented accordingly.

1. Lawfulness of Processing (Art. 6 GDPR)

The processing of audio and video recordings by Aliru GmbH is carried out exclusively on behalf of its clients. The clients are responsible for ensuring compliance with the legal requirements and are obliged to obtain the consent of the meeting participants. Sally, the AI-powered meeting documentation tool, informs all attendees upon joining the meeting of its presence and provides a link to the applicable privacy notice.

As a data processor within the meaning of Article 28 GDPR, Aliru GmbH acts solely on the instructions of the client, who assumes the role of data controller.

2. Transparency and Duty to Inform (Art. 12–14 GDPR)

Aliru GmbH ensures that data subjects are transparently informed about the data processing activities. This is achieved through the following measures:

- Automatic notification of all meeting participants by Sally
- Provision of a privacy notice via a link shared in the meeting chat
- Users may object to the processing by disabling the software during the meeting

3. Processing of Personal Data

The software processes the following categories of data:

- Spoken language (transcripts)
- Metadata (such as date, time, meeting ID, participant list – if provided)
- Video recordings (if enabled, to support transcription)

Aliru GmbH itself does not have access to the content of meetings or to video recordings. All data is stored in encrypted form and is accessible exclusively to the respective client.

4. Data Processing on Behalf of the Controller and Responsibility (Art. 28 GDPR)

Aliru GmbH acts as a data processor and processes personal data exclusively on the instructions of the data controller. This relationship is governed by a data processing agreement (DPA), which includes the following key provisions:

- Data processing is carried out exclusively within the European Union (preferably in Germany).
- Clients retain full control over their data and can manage or delete it at any time (Aliru GmbH does not back up or independently store any data).
- Sub-processors are listed in an annex to the DPA and are subject to the same data protection obligations.

5. Data Security Measures

The software complies with the requirements of Article 32 GDPR on the security of processing through the implementation of appropriate technical and organizational measures (TOMs), including:

- Access control: Hosting is provided in EU-based data centers certified under ISO 27001.
- Access authorization: Only authenticated and authorized client accounts may access the system.
- Encryption: AES-256 encryption is applied to data at rest; TLS/SSL is used for data in transit.
- Logging: All access and modifications are comprehensively logged to ensure traceability.
- Data deletion policy: Data is automatically deleted in accordance with the retention periods defined by the client.

6. Data Retention and Erasure (Art. 5(1)(e) GDPR)

Aliru GmbH does not retain any data beyond the duration specified by the client. Clients have full control to manage and delete transcripts and video recordings at their discretion. Aliru GmbH does not perform automatic deletion but instead ensures that clients maintain full authority over their data.

7. Notification of Personal Data Breaches (Art. 33, 34 GDPR)

The data processing agreement (DPA) includes clear provisions regarding the notification of personal data breaches. These include:

- An obligation on the processor to notify the controller within 24 hours of becoming aware of a breach.
- Detailed requirements for the notification, including a description of the incident, categories of data affected, root causes, and remedial measures taken.
- Assistance to the controller in fulfilling the obligation to notify the supervisory authority.

Conclusion

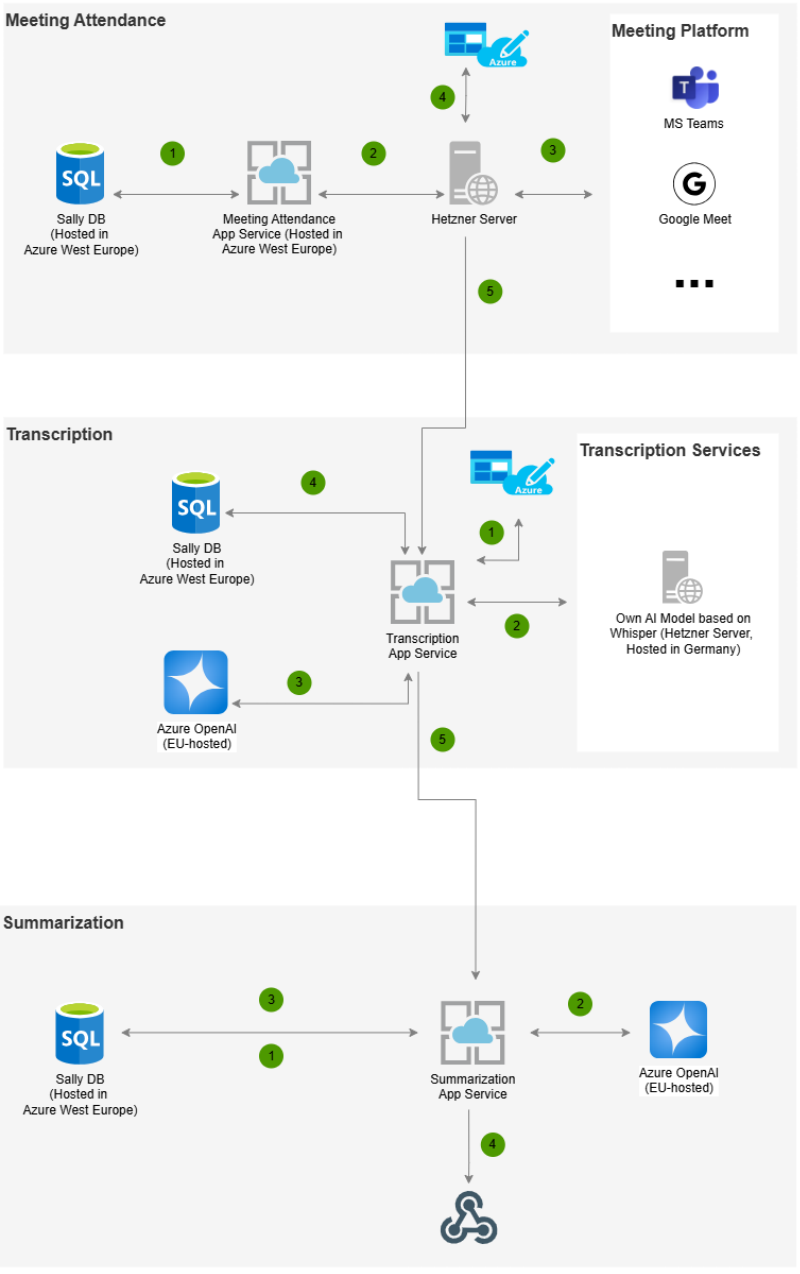
Aliru GmbH has implemented comprehensive measures to ensure GDPR-compliant data processing. In particular, clear contractual arrangements, high security standards, and a strong commitment to transparency form the basis for compliance. Clients retain full control over their data, and processing takes place exclusively within the EU. Accordingly, the processing activities are deemed to be in compliance with the GDPR.

Additional Note

Aliru GmbH is committed to transparency and trustworthy partnerships. We are therefore prepared, at the client's request, to participate in a structured due diligence process and to enter into a corresponding agreement. The objective is to enable a thorough assessment of our data protection and security measures and to support the client as effectively as possible in fulfilling their compliance and risk assessment obligations.

Aliru GmbH
Julian Kissel
CEO

SALLY



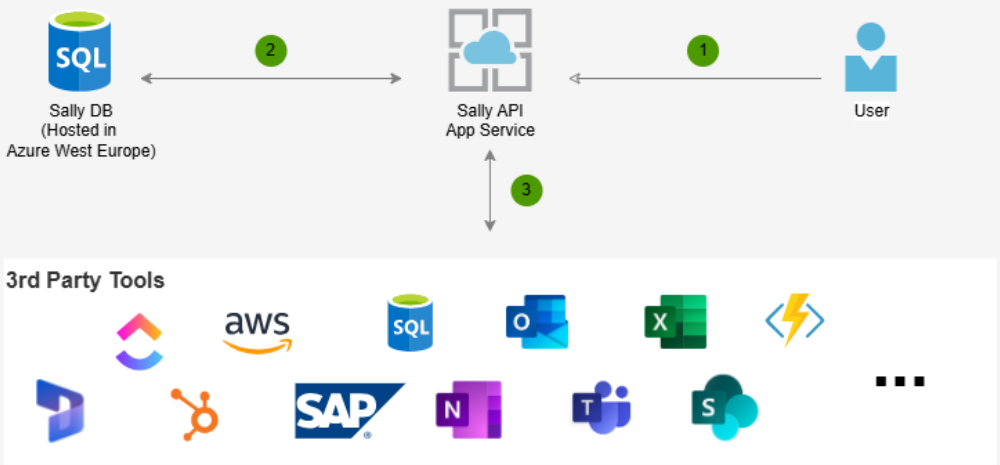
1. The Meeting Attendance Service uses the Sally DB data to check whether attendance at a meeting is expected. Both systems are hosted in Azure in the 'West Europe' data centre.
2. If a meeting has been found that Sally should attend, a new Hetzner node is started in our Kubernetes cluster and the meeting 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.

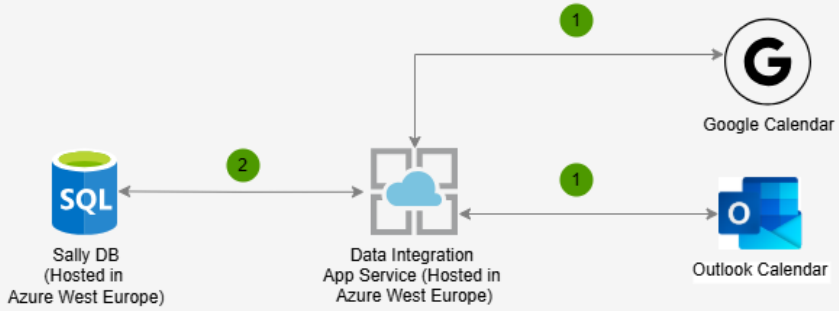
SALLY

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).