

## **Data Processing Agreement**

*(pursuant to Article 28 of the General Data Protection Regulation – GDPR)*

### **Between**

Aliru GmbH  
Julius-Hatry-Straße 1  
68163 Mannheim

– hereinafter referred to as the “Processor” –

### **and**

Name

Street & Number

Postal Code & City

– hereinafter referred to as the “Controller” –

---

### **Preamble**

This Agreement is concluded pursuant to Article 28 of the General Data Protection Regulation (GDPR) and governs the processing of personal data by the Processor on behalf of the Controller. The Processor provides AI-based software that transcribes and analyzes conversations in online meetings. The Controller determines the use of the software, in particular the content to be processed, and is responsible for ensuring compliance with data protection regulations vis-à-vis the participants of the meetings.

This Data Processing Agreement (DPA) is concluded in connection with the main contract for the use of the AI services “Sally” between the Processor and the Controller, which is concluded by the order via [www.sally.de](http://www.sally.de) and the order confirmation.

---

### **§ 1 Matter of the Processing (Article 28 (3) GDPR)**

#### **1. Processing:**

The Processor shall process personal data on behalf of the Controller for the purpose of transcribing and analyzing conversations during online meetings. The processing is carried out to provide the AI-supported functionalities in accordance with the services contractually agreed upon.

#### **2. Duration of the Processing:**

The processing shall be carried out for the duration of the principal agreement or until the termination of the contractually agreed services.

### **3. Categories of Personal Data:**

Conversation data (including recorded audio or video data), names, contact details, as well as other content data provided during the course of the conversations.

### **4. Categories of Data Subjects:**

Participants of the recorded meetings and customers of the Controller, insofar as they are subject to personal data processing within the scope of the agreement.

---

## **§ 2 Duties of the Processor (Article 28(3a–h) GDPR)**

### **1. Data Processing**

The Processor shall process personal data exclusively within the scope of the purposes contractually agreed upon.

### **2. Confidentiality**

The Processor shall ensure that all persons authorized to process personal data are bound by confidentiality obligations and have received appropriate training (Article 28(3b) GDPR).

### **3. Security Measures**

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR. These measures shall be reviewed regularly and adapted to reflect technological developments.

### **4. Assistance to the Controller**

The Processor shall assist the Controller in fulfilling its obligations under Articles 12 to 22 and Articles 32 to 36 GDPR. This includes, in particular:

- a) Promptly notifying the Controller of any personal data breaches falling within the Processor's area of responsibility.
- b) Providing the necessary information and assistance in conducting data protection impact assessments.
- c) Fulfilling information obligations towards supervisory authorities or data subjects, as instructed by the Controller.
- d) The prompt processing of data subject requests in accordance with Articles 12-23 of the GDPR, at the latest within 5 working days of receipt of the request, by providing all necessary information and technical support.

### § 3 Rights and Obligations of the Controller

#### 1. Responsibility for Data Processing

The Controller shall remain solely responsible for the lawfulness of the processing of personal data, including the obtaining of any required consents or ensuring other legal bases pursuant to Article 6 GDPR, as well as for safeguarding the rights of data subjects (Article 4(7) GDPR).

#### 2. Duty to Inform the Processor

The Controller shall inform the Processor without undue delay of any errors, violations, or other circumstances that may affect the Processor's compliance with the GDPR.

#### 3. Provision of Necessary Information

The Controller shall provide the Processor with all information necessary for the proper performance of this Agreement and for compliance with data protection requirements.

#### 4. Handling of Data Subject Requests

If data subjects exercise their rights under Articles 15 to 22 GDPR (e.g., access, rectification, erasure, data portability) directly with the Processor, the Processor shall promptly forward such requests to the Controller. The Controller remains responsible for responding to and fulfilling such requests. The Processor shall assist the Controller in responding to such requests, where required and in accordance with the terms agreed upon in this Agreement.

---

### § 4 Audit and Control Rights of the Controller (*Article 28(3h) GDPR*)

#### 1. Right to Audit and Inspect:

The Controller shall have the right to verify the Processor's compliance with data protection requirements. Audits and inspections may be conducted following prior written notice with a minimum notice period of 14 days and during regular business hours. In doing so, the Controller shall take into account the legitimate business interests of the Processor, in particular trade and business secrets as well as security measures. The statutory control and investigation powers of the competent supervisory authorities, in particular under Article 58 of the GDPR, remain unaffected. The processor shall cooperate with the supervisory authority upon request in accordance with Article 31 of the GDPR.

#### 2. Restricted Access to Sensitive Systems:

If the systems subject to inspection are sensitive technical or security-critical environments, the Processor may limit access to other appropriate evidence (e.g., certifications, audit reports by independent third parties) in order to protect the integrity and confidentiality of the systems.

### **3. Assistance with Inspections:**

The Processor shall assist the Controller in the conduct of audits and inspections by providing the necessary information and documentation (e.g., security concepts, logs). As a general rule, each party shall bear its own costs for audits and the provision of evidence. If the Controller initiates more than one audit per year, the Processor may charge a reasonable fee for each additional audit.

### **4. Evidence of Measures:**

The Processor shall demonstrate the implementation of the technical and organizational measures pursuant to Article 32 GDPR by providing appropriate evidence, including in particular:

- a) Certifications (e.g., ISO 27001, where applicable),
- b) Audit reports by independent third parties,
- c) Internal documentation relating to security measures.

---

## **§ 5 Right to Issue Instructions by the Controller (*Article 28(3a) GDPR*)**

### **1. Principle:**

The processor shall process personal data only on documented instructions from the controller. This also includes the transfer of personal data to a third country or to an international organisation, unless he is obliged to do so under Union law or the law of a Member State to which he is subject. In such a case, the processor shall inform the controller of these legal requirements prior to processing, unless the relevant law prohibits such notification on grounds of important public interest. The controller shall be entitled to issue or adapt instructions during the term of the contract. Instructions that significantly expand or modify the scope of the contractually agreed services require a separate agreement.

### **2. Form of Instructions:**

- a) Instructions from the Controller shall generally be given in writing or in text form (e.g., via email).
- b) In urgent cases, instructions may be given orally but must be confirmed in writing or electronically without undue delay.

### **3. Review of Instructions:**

The Processor shall review the instructions issued by the Controller to determine whether they can be implemented and whether they fall within the scope of the agreed services. If the Processor is unable to comply with an instruction or considers it to be unlawful, the Processor shall inform the Controller without undue delay.

### **4. Deadline for instructions:**

The processor shall implement the controller's instructions without delay. If implementation is not possible within a short period of time, the parties shall agree on an appropriate deadline in each individual case. In doing so, the controller shall take into account the technical and organisational framework conditions of the processor.

**5. Documentation:**

The Processor shall document all instructions, modifications, and corrections issued in connection with the use of the AI service “Sally.” Such documentation shall be retained for the duration of the contractual relationship and beyond, in accordance with statutory retention obligations.

**6. Liability for Deviations from Instructions:**

The Processor shall be liable for damages resulting from processing that is not in accordance with instructions, or from breaches of the GDPR, insofar as such acts or omissions fall within the Processor’s area of responsibility. Liability shall be excluded if the damage occurs despite appropriate security measures and without fault on the part of the Processor - particularly in the case of misuse by third parties without a breach of the security measures required under Article 32 GDPR or as a result of actions by the Controller.

---

**§ 6 Engagement of Sub-Processors (*Articles 28(2) and 28(4) GDPR*)**

**1. Permissibility of Engaging Sub-Processors:**

The engagement of sub-processors for the processing of personal data is only permitted with the prior written authorization of the Controller, unless such sub-processors have already been named in the original agreement and the following conditions for the use of subcontractors are met. The Processor shall inform the Controller in a timely manner before engaging a new sub-processor and shall provide essential information about the subcontracting, including the nature of the processing, the name of the sub-processor, and the planned security measures.

**2. Data Protection Obligations of Sub-Processors:**

The Processor shall ensure that all sub-processors are subject to the same data protection obligations as those set forth in this Agreement between the Controller and the Processor. In particular, it shall be ensured that the sub-processors:

- a) implement technical and organizational measures to protect personal data that are equivalent to those of the Processor,
- b) are bound by confidentiality obligations, and
- c) comply with all relevant obligations arising from this Agreement.

### **3. Sub-Processors Engaged:**

An up-to-date list of the sub-processors engaged by the Processor is provided in Annex 3. Any changes or additions to this list shall be communicated to the Controller in due time to allow the Controller to raise objections.

### **4. Liability of the Processor:**

The Processor shall be liable for the acts and omissions of its sub-processors as if they were its own. The Processor shall ensure that the sub-processor complies with all data protection obligations and shall indemnify the Controller for any violations caused by the sub-processor.

---

## **§ 7 Technical and Organizational Measures (*Article 32 GDPR*)**

### **1. General Security Measures:**

The technical and organizational measures to ensure an appropriate level of protection when using the AI software “Sally” are described in Annex 1 to this Agreement. These measures are designed to safeguard personal data and include, in particular:

- Access controls (ensuring that only authorized individuals have access to personal data),
- Data backup and encryption.
- Access controls (ensuring that only authorized individuals have access to personal data),
- Data backup and encryption,
- Prevention of unauthorized processing and access to the data,
- Ensuring the integrity and availability of the data,
- Monitoring and logging of processing activities. These measures apply to the software environment and the infrastructure used to provide the AI services, as well as to administrative access control to personal data.

### **2. Review and Adjustment of Measures:**

The Processor shall ensure that the technical and organizational measures described in Annex 1 are regularly reviewed, evaluated, and updated as necessary to maintain the continuous protection of personal data. This is carried out in particular with regard to technological developments and the risks posed to the rights and freedoms of the data subjects.

---

## **§ 8 Data processing and storage within the EU**

**1. Data Processing and Storage:**

The processing of personal data in connection with the use of the AI services is carried out in accordance with the Processor's privacy policy, available at [www.sally.io](http://www.sally.io). The Processor processes video and audio recordings strictly in accordance with the Controller's instructions and does not have access to the content. Recordings are stored in encrypted form and retained only for the agreed duration. No disclosure to third parties or independent use by the Processor takes place.

**2. Location of Data Processing:**

The processing and storage of personal data in the context of AI usage occurs exclusively within the EU, preferably in Germany. No transfer to third countries takes place.

**3. No Data Transfers to Third Countries:**

No personal data is transferred to third countries. Should such a transfer be required in individual cases, it will only take place in compliance with the applicable requirements of the GDPR and in coordination with the Controller.

---

**§ 9 Notification of Personal Data Breaches (Articles 33 and 34 GDPR)**

**1. Notification Obligation of the Processor:**

The Processor shall inform the Controller without undue delay, but no later than 24 hours after becoming aware, of any personal data breach that occurs in the context of processing carried out on behalf of the Controller. This applies in particular where the data breach is likely to result in a risk to the rights and freedoms of the data subjects.

**2. Content of the Notification:**

The notification must include the following information:

- A description of the nature of the personal data breach,
- The categories and number of personal data records affected, as well as the number of affected individuals,
- A description of the suspected causes of the breach,
- The measures already taken or planned by the Processor to address the breach and to mitigate its possible adverse effects and associated risks,
- Where applicable, a recommendation regarding notification of the affected data subjects, if necessary to safeguard their rights and freedoms.

**3. Cooperation in Notification to Supervisory Authorities:**

The Processor shall support the Controller in notifying the competent supervi-

sory authority, if required. For this purpose, the Processor shall provide all necessary information to ensure that the Controller can fulfill its obligations under Article 33 GDPR.

---

## **§ 10 Deletion and Return of Data (Article 28(3g) GDPR)**

### **1. Deletion and Return:**

Upon termination of the main contract, and at the latest within 30 days after the end of the contract, the Processor shall delete all personal data processed on behalf of the Controller or, at the Controller's discretion, return it in full in a commonly used, machine-readable format. This does not apply to data that the Processor is legally obliged to retain.

### **2. Confirmation of Deletion:**

The Processor shall confirm in writing to the Controller that all personal data has either been deleted or returned. This confirmation shall be provided no later than 30 days after deletion or return.

### **3. Exceptions:**

If the processor is required by Union law or the law of a Member State to which it is subject to retain personal data beyond the termination of the contract (e.g. for tax or accounting purposes), the processor shall inform the client thereof and ensure that such data is blocked in accordance with the relevant legal provisions so that no unauthorised processing takes place.

---

## **§ 11 Liability and Compensation for Damages (Art. 82 GDPR)**

### **1. Liability of the Processor:**

The Processor shall be liable for any damage resulting from the processing of personal data in a manner not in accordance with instructions, provided that such damage is due to a violation of the provisions of the GDPR or the contractual obligations set forth in this Agreement. This includes, in particular, unlawful processing, loss, or unauthorized disclosure of personal data.

### **2. Liability of the Controller:**

The Controller remains responsible for the lawfulness of the processing of personal data and shall ensure that such processing is based on a valid legal basis pursuant to Article 6 GDPR. The Controller shall also be liable for ensuring the proper safeguarding of the rights of data subjects.

### **3. Limitation of Liability:**

The Processor's liability shall be limited to direct damages caused by a breach of

contractual obligations. Liability for consequential damages, lost profits, or indirect damages is excluded, unless such damage results from intentional misconduct or gross negligence on the part of the Processor.

**4. Compensation for Damages:**

Both parties are obligated to promptly inform each other of any damages related to the processing of personal data. The parties undertake to mitigate any damage to the extent reasonably possible. Claims for damages may only be asserted if the party responsible for the damage has violated its contractual obligations or the provisions of the GDPR intentionally or with gross negligence.

**5. Cooperation by the Controller:**

The Controller agrees to provide all necessary information and to cooperate with the Processor in the event of a claim for damages by data subjects or supervisory authorities, in order to clarify and, where possible, avert liability.

---

**§ 12 Prohibition of Duplication or Disclosure of Data**

**1. Data Processing:**

The Processor is not authorized to copy, reproduce, store, or otherwise process the Controller's personal data unless explicitly permitted by this agreement or by the Controller's written instruction.

**2. No AI Training with User Data:**

The data provided by the Controller and processed through the Sally app must not be used for training AI models. Use of the data by the Processor for its own business purposes, including non-personal data, is expressly excluded.

**3. Unauthorized Disclosure:**

Any unauthorized disclosure, sale, or use of the data—especially for the Processor's own purposes or those of third parties—is strictly prohibited.

**4. Consequences of Breach:**

In the event of a breach of these provisions, the Controller is entitled to terminate the contract without notice and to assert claims for damages.

---

**§ 13 Record of Processing Activities (Art. 30 GDPR)**

**1. Obligation to Maintain a Record:**

The Processor undertakes to maintain a record of all processing activities carried out on behalf of the Controller in accordance with Article 30(2) GDPR. This record shall include all essential details regarding the processing operations, including

the purposes of processing, categories of personal data and data subjects, and the technical and organizational measures (TOMs) implemented.

**2. Availability of the Record:**

Upon request by the Controller, the Processor shall provide a copy of or access to the record of processing activities, insofar as necessary to demonstrate compliance with data protection regulations.

**3. Controller's Obligations:**

The Controller remains responsible for maintaining its own record of processing activities in accordance with Article 30(1) GDPR, which must also include the processing activities carried out by the Processor on its behalf.

**4. Cooperation with Supervisory Authorities:**

The Processor shall support the Controller in fulfilling obligations towards supervisory authorities, in particular by providing information from the record of processing activities where required to meet legal obligations.

**5. Duty to Update:**

The Processor commits to promptly updating the record in the event of changes or additions to processing activities and to informing the Controller of any significant modifications.

---

**§ 14 Insolvency of the Controller**

**1. Notification Obligation of the Controller:**

The Controller is obliged to inform the Processor without undue delay if insolvency proceedings are filed for or opened against its assets, or if comparable proceedings such as enforcement measures, seizures, or attachments take place.

**2. Continuation of Processing in Case of Controller's Insolvency:**

In the event of the Controller's insolvency, the Processor is not obligated to continue the agreed processing of personal data if, due to the insolvency, such continuation becomes impossible or the Controller is no longer able to fulfill its contractual obligations. Nevertheless, the Processor remains bound to protect the personal data in accordance with applicable data protection regulations.

**3. Return or Deletion of Personal Data in the Event of Insolvency:**

In the event of the Controller's insolvency, the Processor undertakes to return or delete, without undue delay, all personal data processed on behalf of the Controller, insofar as this is legally permissible. If the return or deletion is not feasible, the Processor shall continue to protect the data in accordance with the contractual agreements and applicable data protection laws.

#### **4. Termination Right of the Processor:**

The Processor is entitled to terminate the contract with immediate effect if the Controller becomes insolvent and the proper performance of the commissioned processing or the protection of personal data can no longer be ensured as a result. In such case, all personal data of the Controller shall be returned or deleted without undue delay, insofar as legally permissible.

---

### **§ 15 Confidentiality Obligations**

#### **1. Duty of Confidentiality:**

The Processor undertakes to treat as strictly confidential all information obtained in the context of this contractual relationship, including personal data and business information of the Controller.

#### **2. Purpose Limitation:**

Confidential information may only be used for the performance of the services expressly agreed in the contract. Disclosure to third parties is permitted only with the prior written consent of the Controller or where legally required.

#### **3. Measures to Ensure Confidentiality:**

The Processor undertakes to implement appropriate technical and organizational measures to safeguard the confidentiality of the information provided at all times.

#### **4. Duration of the Confidentiality Obligation:**

The obligation of confidentiality shall remain in force for an indefinite period, even after termination of the contractual relationship.

#### **5. Exceptions:**

The confidentiality obligation shall not apply to information

- a) which was demonstrably known to the Processor prior to its disclosure,
  - b) which is publicly available or becomes publicly known without breach of this Agreement, or
  - c) which must be disclosed due to a legal obligation or official order.
- 

### **§ 16 Duty of confidentiality pursuant to § 203 StGB (German Criminal Code)**

#### **1. Condition for activation:**

This § 16 shall only apply in a supplementary manner if the client confirms in text form that he is bound by professional secrecy within the meaning of § 203 StGB. Otherwise, the general confidentiality provisions of § 15 AVV shall apply exclusively.

**2. Scope of application / professional secrecy:**

Insofar as the client is subject to a statutory duty of confidentiality pursuant to Section 203 StGB, the processor acknowledges that, in the course of providing services, it may become aware of information that is protected as professional secrecy within the meaning of Section 203 StGB (in particular such information pursuant to Section 43a BRAO in conjunction with BORA, § 57 StBerG, § 43 WPO, § 39a PAO; “professional secrets”).

**3. Assumption of the duty of confidentiality / principle:**

The processor undertakes the client's duty of confidentiality in accordance with Section 203 of the German Criminal Code (StGB). It shall maintain confidentiality regarding all professional secrets that become known to it in the course of or in connection with its activities, protect them from unauthorized access, and only obtain knowledge of them to the extent necessary for the proper performance of the contract (“need-to-know”).

**4. Obligation of employees:**

The processor shall ensure that all employees and any subcontractors who have access to the client's data in the course of processing are expressly obliged to comply with the duty of confidentiality in accordance with Section 203 of the German Criminal Code (StGB).

**5. Disclosure only in case of legal obligation:**

Professional secrets shall only be disclosed on the instructions of the client or if required by mandatory Union law or the law of a Member State. In this case, the processor shall inform the client in advance of the legal requirements, unless this is prohibited by law, and shall limit the disclosure to the minimum necessary; such access shall be logged.

**6. Duration, return, deletion:**

The duty of confidentiality shall apply indefinitely and beyond the end of the contract. After the end of the contract, documents and data carriers containing professional secrets shall be securely deleted in accordance with the client's instructions; statutory retention obligations shall remain unaffected; in this case, the data shall be blocked.

**7. Priority of this provision:**

This special provision takes precedence over the general confidentiality obligations of this contract, where applicable.

**8. Obligations that remain unaffected:**

Further data protection obligations (in particular those arising from the GDPR and the AVV) remain unaffected by this provision.

## § 17 Termination of the Agreement

### 1. Ordinary Termination:

The contract, including the subscription, may be terminated by either party up to one day prior to the renewal of the subscription, unless otherwise agreed in writing.

### 2. Extraordinary Termination:

The right to extraordinary termination for good cause remains unaffected. Good cause shall be deemed to exist in particular if:

- a) either party repeatedly or materially breaches contractual or statutory obligations, especially regarding the use of the provided AI,
- b) insolvency proceedings are opened over the assets of either party or such proceedings are applied for, or
- c) actions or omissions by either party render compliance with the GDPR or other legal requirements no longer feasible.

### 3. Termination of Subscription:

Upon termination of the contract, the subscription shall also end, and the Processor shall no longer be entitled to use the provided data or services as of the termination date, unless a legal obligation to retain such data continues to apply.

### 4. Consequences of Termination:

- a) Upon termination of the contractual relationship, the Processor is obliged to delete all data collected during the processing and use of personal data in accordance with data protection requirements, unless a legal retention obligation exists.
- b) The Processor shall confirm the deletion of the data in writing.

---

## § 18 Place of Jurisdiction and Applicable Law

### 1. Applicable Law:

The law of the Federal Republic of Germany shall apply, to the exclusion of international private law and the United Nations Convention on Contracts for the International Sale of Goods (CISG). In the event of any conflict, discrepancy, or inconsistency between the English and German versions of this Agreement, the German version shall prevail and be binding.

### 2. Place of Jurisdiction:

For all disputes arising out of or in connection with this contract, the exclusive place of jurisdiction shall be the registered office of the Processor (Mannheim),

provided that the Controller is a merchant, a legal entity under public law, or a special fund under public law.

---

### § 19 Severability Clause

1. Should individual provisions of this Agreement be or become wholly or partially invalid or unenforceable after the conclusion of the Agreement, the validity of the remaining provisions shall remain unaffected.
  2. In place of the invalid or unenforceable provision, a valid and enforceable provision shall apply which most closely reflects the economic purpose of the invalid provision.
  3. The same shall apply in the event of any contractual omissions.
- 

### Annexes

1. Technical and Organisational Measures (Annex 1)
  2. Record of Processing Activities of the Processor (Annex 2)
  3. Subprocessors Employed (Annex 3)
  4. Data Protection Impact Assessment (DPIA) for the AI Solution (Annex 4)
  5. AI Compliance Declaration in accordance with the EU AI Act (Annex 5)
  6. Compliance with Regulation (EU) 2024/1689 – AI Act (Annex 6)
  7. Process descriptions for the use of Sally (Annex 7)
- 

**Signatures**

Place, Date: \_\_\_\_\_

*Julian Kissel*

---

**Processor**

Julian Kissel  
CEO

**Controller**

Name  
Position (authorized representative)

## **Annex 1: Technical and Organisational Measures**

### **1. Access Control (Hosting Location)**

Physical access control is ensured by our cloud hosting providers within the EU (Microsoft Azure) and in Germany (Hetzner – strongly preferred). These providers are obligated to operate data centers in accordance with high security standards (e.g., ISO 27001) and to protect them against unauthorized access.

### **2. Access Control (Logical)**

Access to the AI application is secured through the following measures:

- **Authentication:** Customers (controllers) integrate the AI into their meetings via registered accounts. Unauthorized access is excluded.
- **Encryption:** All data transmissions are conducted exclusively through encrypted channels (e.g., HTTPS).
- **Access Logging:** All access requests are logged and monitored for potential misuse patterns.
- **Access to Stored Video Recordings:** Access to stored video content is restricted to authorized users based on a defined access control policy.
- **Encrypted Storage:** Stored videos are encrypted and can only be decrypted by authorized entities.
- All workstation computers are centrally managed via Microsoft Intune, ensuring consistent implementation of security policies and device configurations.
- In addition, Microsoft Defender for Endpoint is active on all devices to provide advanced threat detection and response.
- Microsoft Defender Antivirus is installed on all end devices and enabled at all times.

### **3. Transfer Control**

Measures to ensure the secure transmission and storage of data include:

- Encryption of data transmissions using TLS 1.3/SSL protocols.
- Logging of all data transfers to ensure traceability.
- Transfer of personal data to third parties only with the prior consent of the controller.

- Use of VPN connections for secure remote access.
- No disclosure of video recordings to third parties without the controller's explicit instruction.
- Processing of video recordings takes place exclusively within designated systems.

#### **4. Input Control**

Measures to ensure the traceability of the processing of personal data:

- Logging of all entries, modifications, and deletions of personal data.
- Documentation of user activities in audit logs.
- Training of employees on proper data processing practices.
- Documentation of access to stored video recordings.
- Transparent labeling of video data processing in system logs.

#### **5. Order Control**

Measures to ensure data processing is conducted solely in accordance with instructions:

- Processing activities are carried out exclusively in accordance with the controller's instructions (Art. 28 GDPR).
- Employee training on the controller's instructions and GDPR compliance.
- Regular internal audits to verify compliance.
- Use of video recordings is limited strictly to transcription purposes, with no storage beyond the agreed retention periods.

#### **6. Availability Control**

Measures to ensure availability and protection against data loss:

- Regular system backups (at least daily).
- Use of redundant systems (e.g., RAID configurations, failover solutions).
- Contingency plans and regular testing of recovery procedures.
- Ensuring that video and other recordings are no longer accessible in any form after deletion has been requested by the controller.

#### **7. Handling of temporary raw data (audio/video recordings)**

- Raw data that is processed exclusively for the purpose of transcription and analysis will be automatically deleted after completion of the respective processing operation.

- Raw data will not be stored beyond the processing time unless the client has expressly requested that the recording be stored.
- Audio and video data stored by the client will only be deleted in accordance with the client's instructions or after the end of the contract in accordance with § 10 AVV.

## **8. Data Separation Requirement**

Measures to ensure separate processing of data for different controllers:

- Logical separation of data through distinct databases or directories.
- Access restrictions based on client-specific (tenant) permissions.
- Strict segregation of development and production environments.
- Video recordings are stored and processed separately for each client.

## **9. Encryption**

Measures to ensure data confidentiality:

- Encryption of stored data using AES-256.
- Use of modern encryption standards for data transmission (e.g., HTTPS).
- Encryption of mobile storage media (e.g., USB sticks, laptops).
- Video recordings are stored in encrypted form (AES-256).
- Access to encrypted data is restricted to designated, authorized entities.

## **10. Measures in the Event of Disruptions and Data Breaches**

- Implementation of an incident management process for reporting and handling data protection incidents.
- Immediate notification of the controller in the event of a data breach, in accordance with Art. 33 GDPR.
- Documentation of security incidents and the corrective actions taken.

## **11. Awareness and Training of Employees**

- Regular training on data protection and information security.
- Confidentiality obligations for all employees with access to personal data.
- Monitoring and enforcement of compliance with security policies by employees.
- Reporting of any incidents, including unauthorized access or unlawful use of video recordings.

These measures are reviewed regularly and adapted to reflect the current state of the art and the requirements of the controller. Any changes or additions to this Annex shall be agreed upon in writing.

## Annex 2: Record of Processing Activities of the Processor (Art. 30(2) GDPR)

No.	Processing Activity	Purpose of Processing	Categories of Data Subjects	Categories of Personal Data	Legal Basis	Recipients (if applicable)	Retention Period	Third-Country Transfer (yes/no)
1	Transcription and Logging of Meetings	Provision of meeting transcripts and summaries	Meeting participants (e.g., customers, business partners, client's employees)	Audio and Video recordings, transcripts, metadata (participants, time, duration)	Art. 6 GDPR (data processing on behalf)	None	30 days after contract termination or upon controller's instruction	No

### Additional Information

- **TOMs (Technical and Organisational Measures):** See Annex 1
- **Data Protection Officer:**  
Name: Norton Engele  
Email address: [privacy@sally.io](mailto:privacy@sally.io)

**Anlage 3: Subcontractors**

<b>Name of Subprocessor</b>	<b>Server Location / Branch</b>	<b>Service Provided</b>	<b>Permanent contract &amp; data processing within the EU</b>	<b>Privacy Policy</b>
Hetzner Online GmbH	Server Location: Germany  Branch: Industriestr. 25, 91710 Gunzenhausen, Deutschland	Cloud infrastructure / web hosting / backups	Yes  EU – Germany	<a href="#">Hetzner Privacy Policy</a>
Microsoft Ireland Operations Limited	Server Location: Netherlands  Branch: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland.	Cloud infrastructure for computing power and storage	Yes  EU – Netherlands	<a href="#">Microsoft Privacy Policy</a>
Amazon Web Services EMEA SARL (AWS)	Server Location: Germany / Ireland	CloudfrontVideo- / audio distribution, origin in Azure (optionally deactivatable)	Yes  EU – Germany / Ireland	<a href="#">AWS Privacy Policy</a>

	Branch: 38 Avenue John F. Kennedy, L-1855 Luxembourg			
DeepL SE	Server Location: Germany Branch: Maarweg 165, 50825 Köln, Deutschland.	AI-powered translations	Yes EU – Germany	<a href="#">DeepL Privacy Policy</a>
Stripe Payments Europe, Limited	Server Location: Ireland Branch: The One Building, 1 Lower Grand Canal Street, Dublin 2, D02 HD59, Ireland	Payment processing and transaction management	Yes EU – Ireland	<a href="#">Stripe Privacy Policy</a>
Strato AG	Server Location: Germany Branch: Pascalstraße 10, 10587 Berlin, Deutschland	Web hosting and infrastructure	Yes EU – Germany	<a href="#">Strato Privacy Policy</a>

Azure OpenAI (Microsoft Ireland Operations Limited)	Server Location. Sweden  Branch: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland.	AI services from OpenAI (provided via Microsoft Azure)	Yes  EU – Sweden	<a href="#">Microsoft Privacy Policy</a>
---	--	--	------------------------	--

## **Annex 4: Data Protection Impact Assessment (DPIA) for the AI Solution**

### **1. Introduction**

This Data Protection Impact Assessment (DPIA) is conducted in accordance with Article 35 of the GDPR for the AI-powered meeting documentation software of the company. The objective is to systematically analyze the risks to data subjects and to define appropriate protective measures.

### **2. Description of Processing**

- **Purpose of Processing:**

Automated transcription, analysis, and summarization of meetings for efficient documentation and follow-up.

- **Personal Data Processed:**

- Spoken language (transcripts)
- Names and contact details of meeting participants (as captured)
- Metadata (date, time, duration, meeting ID)
- Video recordings of meetings to support transcription
- Data Subjects: Participants of meetings (customers, partners, employees).
- Data Sources: Live audio and video recordings from online meetings.
- Processors Involved: Microsoft Azure (hosting), Azure OpenAI (text analysis)

### **3. Assessment of Necessity and Proportionality**

- The processing is carried out to provide efficient meeting documentation and to replace manual note-taking.
- Proportionality is ensured, as only relevant data is processed.

- The processing is based on the consent of participants or on legitimate interest pursuant to Article 6(1)(f) GDPR.

#### **4. Assessment of Risks to the Rights and Freedoms of Data Subjects**

##### **Potential Risks:**

- Unauthorized access to transcripts, video recordings, and metadata
- Misuse or misinterpretation of the data
- Insufficient transparency for data subjects
- Risks arising from the use of external AI service providers

#### **5. Measures to Mitigate Risks**

- **Technical and Organizational Measures (TOMs):**

- Encryption of transcripts, video recordings, and stored data
- Access restrictions and role-based permissions
- For users from the European Union (EU), all data traffic remains entirely within the EU data border. No personal data is transferred or processed outside the European Union
- Pseudonymization of sensitive data
- Ensuring that video and other recordings are no longer available in any form once deletion has been initiated by the data controller
- Transparent user information regarding the recording and processing of video content
- Regular data protection and security audits
- Further detailed measures can be found in Annex 1: Technical and Organizational Measures

- **Specification of deletion periods for raw data:**

- Temporary raw data required for transcription and analysis will be deleted immediately after processing is complete.
- Permanent storage of raw data will only take place at the express request of the client.
- In all other respects, the deletion policy set out in the DPA (§ 10) applies.
- Contractual safeguards:
  - Conclusion of data processing agreements (DPA) with all subcontractors.
  - Ensuring GDPR compliance of external service providers.

- **Contractual Safeguards:**

- Conclusion of data processing agreements (DPAs) with all subcontractors
- Ensuring GDPR compliance of external service providers

- **Data Subject Rights:**

- Transparent information on data processing
- Implementation of deletion periods and rights to object

## 6. Conclusion

After assessing the risks and implemented measures, the processing is deemed GDPR-compliant and poses an acceptable risk to the data subjects. The Data Protection Impact Assessment is reviewed and updated on a regular basis.

## Annex 5: AI Conformity Declaration in accordance with the EU AI Act

### 1. Introduction

This declaration is issued in accordance with Regulation (EU) 2024/1689 (AI Act) and outlines the conformity of the AI-powered meeting documentation software with the regulation's requirements. The goal is to ensure transparency regarding the AI technologies used and their impact on affected individuals.

### 2. Description of the AI System

- **Function:** Automatic transcription, summarization, and analysis of spoken content in meetings
- **Data Processing:** Processing of speech and video recordings to improve transcription quality
- **Purpose of Processing:** Documentation and follow-up of meeting content
- **Deployed AI Technologies:** Speech recognition and text analysis through specialized models

### 3. Classification under the AI Act

The system is not classified as high-risk AI under Annex III of Regulation (EU) 2024/1689, as it does not perform biometric identification, behavioral analysis, or automated decision-making with significant effects on data subjects. The video recordings are used solely to support transcription and are not analyzed for facial expressions, emotions, or behavior.

### 4. Measures to Ensure Compliance

- **Transparency:** Users are informed about the use of AI and its functioning
- **Data Protection & Security:** Processing is conducted solely within the EU; data is encrypted, access is restricted, and regular audits are performed (see Annex 1: Technical and Organizational Measures)
- **Contractual Safeguards:** Data processing agreements (DPAs) are in place with subcontractors in accordance with the GDPR
- **Usage Limitations:** No use of data for model improvement or training purposes

## 5. Conclusion

The AI system complies with the requirements of the AI Act and does not constitute a high-risk application. The measures implemented ensure data protection, transparency, and security for affected individuals. This declaration is reviewed and updated regularly to remain aligned with evolving regulatory requirements.

## **Annex 6: Compliance with Regulation (EU) 2024/1689 (AI Act)**

### **1. Risk Management and Compliance**

The processor undertakes to comply with the provisions of Regulation (EU) 2024/1689 (AI Act). This includes, in particular, conducting a risk assessment of the AI system in accordance with the Regulation's requirements and implementing appropriate risk mitigation measures.

### **2. Transparency and Traceability**

The processor ensures that the AI system is designed in a way that enables traceable and documented decision-making processes affecting data subjects. Documentation on the functionality of the AI will be made available upon request, unless trade secrets or intellectual property rights prevent disclosure.

### **3. Security and Robustness**

The processor guarantees that the AI system is subject to technical and organizational security measures to prevent malfunctions, unauthorized access, and manipulation. These measures are detailed in **Annex 1: Technical and Organizational Measures**.

### **4. Non-Discrimination and Fairness**

The processor takes appropriate steps to avoid systematic bias in the AI model that could lead to discrimination. This includes regular audits of training data and model outputs.

### **5. Ongoing Monitoring and Reporting**

The processor regularly reviews the AI system to ensure compliance with Regulation (EU) 2024/1689 and documents all relevant audits and findings. Significant changes to the AI system or newly identified risks will be reported promptly to the controller.

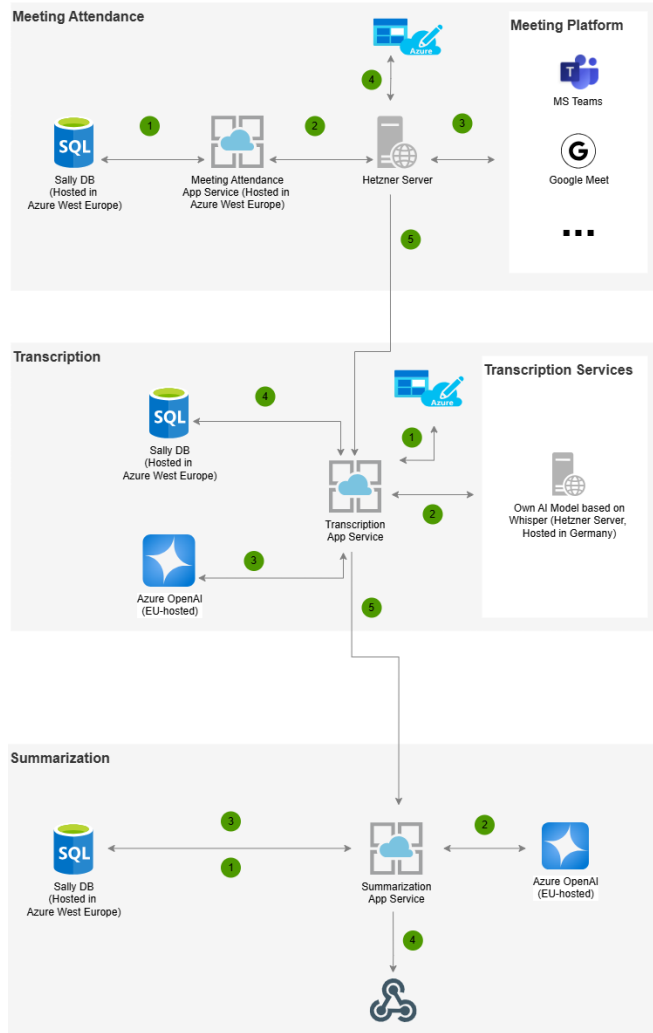
### **6. Cooperation with the Controller**

The processor supports the controller in fulfilling their obligations under Regulation (EU) 2024/1689, particularly regarding requests from supervisory authorities or data subjects.

### **7. References to Existing Documentation**

Additional provisions concerning data processing, security, and responsibilities are outlined in the following annexes:

## Annex 7: Process descriptions for the use of Sally

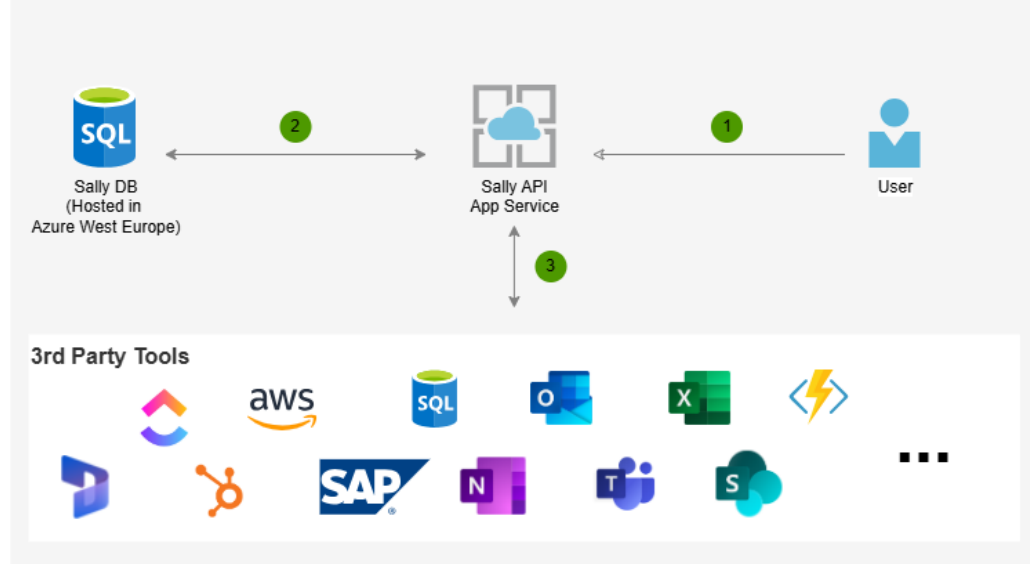


- 1 The Meeting Attendance Service uses the Sally DB data to check whether attendance at a meeting is expected. Both systems are hosted in Azure in the 'West Europe' data centre.
- 2 If a meeting has been found that Sally should attend, a new Hetzner node is started in our Kubernetes cluster and the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

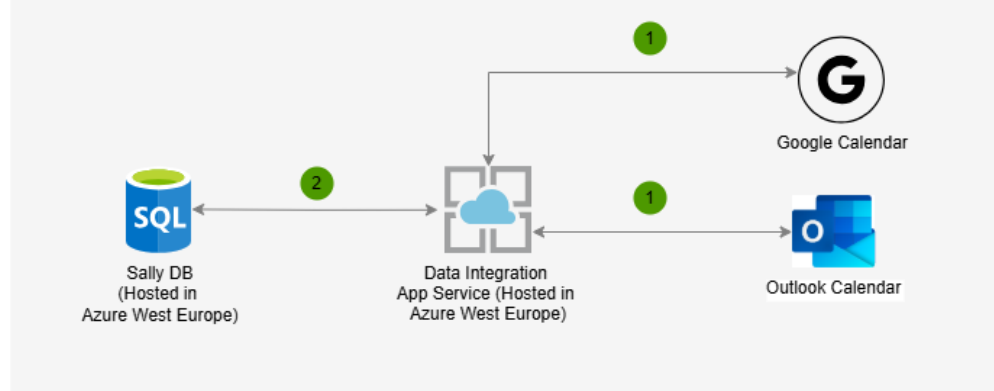
- 1 Based on the HTTPS request, the Summarisation Service, which is hosted within the EU (Azure data centre: West Europe), loads from the Sally DB via encrypted connection the information from the transcription and also all additional data known for the appointment (subject, description, participant, 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.

### 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).