Auftragsverarbeitungsvertrag
(gemäß Art. 28 Datenschutz-Grundverordnung – DSGVO)

Zwischen
Aliru GmbH
Julius-Hatry-Straße 1
68163 Mannheim

– im Folgenden „Auftragsverarbeiter“ –

und

Name

Straße & Hausnummer

PLZ & Ort

– im Folgenden „Auftraggeber“ –

Präambel

Dieser Vertrag wird gemäß Art. 28 DSGVO geschlossen und regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Auftraggebers. Der Auftragsverarbeiter stellt eine KI-basierte Software zur Verfügung, die Gespräche in Online-Meetings transkribiert und analysiert. Der Auftraggeber entscheidet über die Nutzung der Software, insbesondere über die Inhalte, die verarbeitet werden, und ist verantwortlich für die Einhaltung der datenschutzrechtlichen Bestimmungen gegenüber den Teilnehmern der Meetings.

Dieser Auftragsverarbeitungsvertrag (AVV) wird abgeschlossen im Zusammenhang mit dem Hauptvertrag über die Nutzung der KI-Dienste „Sally“ zwischen dem Auftragsverarbeiter und dem Auftraggeber, welcher durch die Bestellung über www.sally.de und die Auftragsbestätigung zustande gekommen ist.

---

§ 1 Gegenstand der Verarbeitung *(Art. 28 Abs. 3 DSGVO)*

1. **Art und Zweck der Verarbeitung:**
   Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers, um Gespräche während Online-Meetings zu transkribieren und zu analysieren. Die Verarbeitung dient der Bereitstellung der KI-gestützten Funktionen gemäß den vertraglich vereinbarten Leistungen.

2. **Dauer der Verarbeitung:**
   Die Verarbeitung erfolgt für die Dauer des Hauptvertrags oder bis zur Beendigung der vertraglich festgelegten Leistungen.

3. **Art der personenbezogenen Daten:**
   Gesprächsdaten (einschließlich aufgezeichneter Audio- oder Videodaten), Namen, Kontaktdaten sowie weitere Inhaltsdaten, die im Rahmen der Gespräche bereitgestellt werden.

4. **Betroffene Personen:**
   Teilnehmer der aufgezeichneten Meetings und Kunden des Auftraggebers, sofern diese im Rahmen der Verarbeitung personenbezogener Daten erfasst werden.

---

§ 2 Pflichten des Auftragsverarbeiters *(Art. 28 Abs. 3 lit. a–h DSGVO)*

1. **Verarbeitung der Daten**
   Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der vertraglich vereinbarten Zwecke.

2. **Vertraulichkeit:**
   Der Auftragsverarbeiter stellt sicher, dass alle Personen, die Zugang zu den personenbezogenen Daten haben, zur Vertraulichkeit verpflichtet sind und geeignete Schulungen erhalten haben (Art. 28 Abs. 3 lit. b DSGVO).

3. **Sicherheitsmaßnahmen:**
   Der Auftragsverarbeiter setzt angemessene technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO sicherzustellen. Diese Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.

4. **Unterstützung des Auftraggebers:**
   Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung seiner Verpflichtungen gemäß Art. 12-22 sowie Art. 32–36 DSGVO. Dies umfasst insbesondere:
   a) Die unverzügliche Meldung von Datenschutzverletzungen, die in den Verantwortungsbereich des Auftragsverarbeiters fallen, an den Auftraggeber.
   b) Die Bereitstellung der notwendigen Informationen und Unterstützung bei der Durchführung von Datenschutz-Folgenabschätzungen.
   c) Die Erfüllung von Informationspflichten gegenüber Aufsichtsbehörden oder betroffenen Personen auf Anweisung des Auftraggebers.
   d) Die unverzügliche Bearbeitung von Betroffenenanfragen gemäß Art. 12-23 DSGVO, spätestens jedoch innerhalb von 5 Werktagen nach Eingang der Anfrage, durch Bereitstellung aller erforderlichen Informationen und technischen Unterstützung.

§ 3 Rechte und Pflichten des Auftraggebers

1. **Verantwortlichkeit für die Datenverarbeitung:**
   Der Auftraggeber ist und bleibt für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich, einschließlich der Einholung erforderlicher Einwilligungen oder der Erfüllung anderer Rechtsgrundlagen gemäß Art. 6 DSGVO sowie der Wahrung der Rechte der betroffenen Personen (Art. 4 Nr. 7 DSGVO).

2. **Informationspflicht gegenüber dem Auftragsverarbeiter:**
   Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich über Fehler, Verstöße oder sonstige Umstände, die die Einhaltung der DSGVO durch den Auftragsverarbeiter beeinträchtigen könnten.

3. **Bereitstellung notwendiger Informationen:**
   Der Auftraggeber stellt dem Auftragsverarbeiter alle Informationen zur Verfügung, die für die ordnungsgemäße Erfüllung des Vertrags und die Einhaltung der Datenschutzanforderungen erforderlich sind.

4. **Umgang mit Anfragen betroffener Personen:**
   Falls betroffene Personen ihre Rechte gemäß Art. 15–22 DSGVO (z. B. Auskunft, Berichtigung, Löschung, Datenübertragbarkeit) direkt gegenüber dem Auftragsverarbeiter geltend machen, leitet der Auftragsverarbeiter diese Anfragen unverzüglich an den Auftraggeber weiter. Der Auftraggeber bleibt für die Bearbeitung und Beantwortung der Anfragen verantwortlich. Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Beantwortung der Anfragen, sofern dies erforderlich ist und nach den vertraglich vereinbarten Regelungen erfolgt.

§ 4 Kontrollrechte des Auftraggebers *(Art. 28 Abs. 3 lit. h DSGVO)*

1. **Audit- und Inspektionsrecht:**
   Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter zu überprüfen. Audits und Inspektionen können nach vorheriger schriftlicher Ankündigung mit einer Frist von mindestens 14 Tagen und während der üblichen Geschäftszeiten durchgeführt werden. Der Auftraggeber hat dabei die berechtigten Geschäftsinteressen des Auftragsverarbeiters, insbesondere Betriebs- und Geschäftsgeheimnisse sowie Sicherheitsmaßnahmen, zu berücksichtigen.
   Die gesetzlichen Kontroll- und Untersuchungsbefugnisse der zuständigen

Aufsichtsbehörden, insbesondere nach Art. 58 DSGVO, bleiben unberührt. Der Auftragsverarbeiter arbeitet auf Anfrage gemäß Art. 31 DSGVO mit der Aufsichtsbehörde zusammen.

2. **Eingeschränkter Zugang bei sensiblen Systemen:**
   Sofern es sich bei den überprüften Systemen um sensible technische oder sicherheitskritische Umgebungen handelt, kann der Auftragsverarbeiter den Zugang auf andere geeignete Nachweise (z. B. Zertifizierungen, Auditberichte durch unabhängige Dritte) beschränken, um die Integrität und Vertraulichkeit der Systeme zu schützen.

3. **Unterstützung bei Kontrollen:**
   Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Durchführung von Audits und Inspektionen, indem er die erforderlichen Informationen und Dokumentationen (z. B. Sicherheitskonzepte, Protokolle) bereitstellt. Grundsätzlich tragen die Parteien ihre eigenen Kosten für Audits und andere Nachweise selbst. Werden durch den Auftraggeber mehrere Audits pro Jahr initiiert, kann der Auftragsverarbeiter ab dem zweiten Audit ein angemessenes Entgelt verlangen.

4. **Nachweis der Maßnahmen:**
   Der Auftragsverarbeiter weist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO durch geeignete Nachweise nach. Dazu zählen insbesondere:
   a) Zertifizierungen (z. B. ISO 27001, soweit zutreffend),
   b) Auditberichte unabhängiger Dritter,
   c) interne Dokumentationen zu Sicherheitsmaßnahmen.

---

§ 5 Weisungsrecht des Auftraggebers *(Art. 28 Abs. 3 lit. a DSGVO)*

1. **Grundsatz:**
   Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Dies umfasst auch die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation, sofern er nicht nach Unionsrecht oder dem Recht eines Mitgliedstaats, dem er unterliegt, zur Übermittlung verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt. Der Auftraggeber ist berechtigt, während der Laufzeit des Vertrags Weisungen zu erteilen oder anzupassen. Weisungen, die den vertraglich vereinbarten Leistungsumfang wesentlich erweitern oder ändern, bedürfen jedoch einer gesonderten Vereinbarung.

2. **Form der Weisungen:**
   a) Weisungen des Auftraggebers erfolgen grundsätzlich schriftlich oder in Textform (z. B. per E-Mail).
   b) In dringenden Fällen können Weisungen auch mündlich erteilt werden, müssen jedoch unverzüglich schriftlich oder elektronisch bestätigt werden.

3. **Prüfung der Weisungen:**
   Der Auftragsverarbeiter prüft die Weisungen des Auftraggebers auf ihre Umsetzbarkeit und darauf, ob sie den vertraglich vereinbarten Leistungen entsprechen. Kann der Auftragsverarbeiter eine Weisung nicht umsetzen oder hält er sie für rechtswidrig, informiert er den Auftraggeber unverzüglich darüber.

4. **Frist der Weisungen:**
   Der Auftragsverarbeiter setzt Weisungen des Auftraggebers unverzüglich um. Ist eine Umsetzung innerhalb kurzer Zeit nicht möglich, stimmen die Parteien die hierfür angemessene Frist im Einzelfall ab. Der Auftraggeber wird dabei die technischen und organisatorischen Rahmenbedingungen des Auftragsverarbeiters berücksichtigen.

5. **Dokumentation:**
   Der Auftragsverarbeiter dokumentiert alle Weisungen, Änderungen und Korrekturen, die im Rahmen der Nutzung der KI "Sally" erfolgen. Diese Dokumentation wird für die Dauer des Vertragsverhältnisses und darüber hinaus gemäß den gesetzlichen Aufbewahrungspflichten gespeichert.

6. **Haftung bei Weisungsabweichung:**
   Der Auftragsverarbeiter haftet für Schäden, die durch eine nicht weisungsgemäße Verarbeitung oder durch Verstöße gegen die Vorgaben der DSGVO entstehen, soweit diese Handlungen oder Unterlassungen in seinem Verantwortungsbereich liegen. Eine Haftung entfällt, soweit der Schaden trotz angemessener Sicherheitsmaßnahmen und ohne eigenes Verschulden des Auftragsverarbeiters entsteht, insbesondere bei Missbrauch durch Dritte ohne Verstoß gegen Sicherheitsmaßnahmen nach Art. 32 DSGVO oder durch Handlungen des Auftraggebers selbst.

---

§ 6 Einsatz von Subunternehmern *(Art. 28 Abs. 2 und 4 DSGVO)*

1. **Zulässigkeit des Einsatzes von Subunternehmern:**
   Der Einsatz von Subunternehmern zur Verarbeitung personenbezogener Daten ist nur mit vorheriger schriftlicher Genehmigung des Auftraggebers zulässig, sofern solche Subunternehmer nicht bereits in der ursprünglichen Vereinbarung benannt wurden und die nachfolgenden Voraussetzungen zum Einsatz von Subunternehmern erfüllt sind. Der Auftragsverarbeiter informiert den

Auftraggeber rechtzeitig vor der Beauftragung eines neuen Subunternehmers und übermittelt ihm wesentliche Details zur Subvergabe, einschließlich der Art der Verarbeitung, des Namens des Subunternehmers und der geplanten Sicherheitsmaßnahmen.

2. **Datenschutzverpflichtungen der Subunternehmer:**
   Der Auftragsverarbeiter stellt sicher, dass alle Subunternehmer denselben Datenschutzverpflichtungen unterliegen, wie sie im vorliegenden Vertrag zwischen dem Auftraggeber und dem Auftragsverarbeiter vereinbart sind. Insbesondere wird gewährleistet, dass die Subunternehmer:
   a) technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten umsetzen, die denjenigen des Auftragsverarbeiters gleichwertig sind,
   b) zur Vertraulichkeit verpflichtet werden und
   c) alle relevanten Verpflichtungen aus diesem Vertrag einhalten.

3. **Eingesetzte Subunternehmer:**
   Eine aktuelle Liste der vom Auftragsverarbeiter eingesetzten Subunternehmer wird in Anlage 3 bereitgestellt. Änderungen oder Ergänzungen dieser Liste werden dem Auftraggeber rechtzeitig mitgeteilt, um ihm die Möglichkeit zu geben, Einwände zu erheben.

4. **Haftung des Auftragsverarbeiters:**
   Der Auftragsverarbeiter haftet für die Handlungen und Unterlassungen seiner Subunternehmer, als ob er diese selbst ausgeführt hätte. Er stellt sicher, dass der Subunternehmer alle datenschutzrechtlichen Verpflichtungen einhält und den Auftraggeber für etwaige Verstöße schadlos hält, sofern der Verstoß durch den Subunternehmer verursacht wurde.

---

§ 7 Technische und organisatorische Maßnahmen *(Art. 32 DSGVO)*

1. **Allgemeine Sicherheitsmaßnahmen:**
   Die technischen und organisatorischen Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus bei der Nutzung der KI-Software "Sally" werden in der Anlage 1 des Vertrages beschrieben. Diese Maßnahmen dienen dem Schutz personenbezogener Daten und umfassen insbesondere:

   - Zugangskontrollen (nur autorisierte Personen haben Zugang zu den personenbezogenen Daten),
   - Datensicherung und -verschlüsselung,
   - Verhinderung der unbefugten Verarbeitung und des unbefugten Zugriffs auf die Daten,

- Sicherstellung der Integrität und Verfügbarkeit der Daten,
- Überwachung und Protokollierung der Verarbeitungsvorgänge.
  Diese Maßnahmen betreffen die Softwareumgebung und die Infrastruktur, die zur Bereitstellung der KI verwendet wird, sowie die administrative Zugriffskontrolle auf personenbezogene Daten.

2. **Überprüfung und Anpassung der Maßnahmen:**
   Der Auftragsverarbeiter stellt sicher, dass die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen regelmäßig überprüft, bewertet und bei Bedarf aktualisiert werden, um den fortlaufenden Schutz der personenbezogenen Daten zu gewährleisten. Dies erfolgt insbesondere im Hinblick auf technologische Entwicklungen und die Risiken für die Rechte und Freiheiten der betroffenen Personen.

---

§ 8 Datenverarbeitung und -speicherung innerhalb der EU

1. **Datenverarbeitung und Speicherung:**
   Die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der KI-Dienste erfolgt gemäß der Datenschutzerklärung des Auftragsverarbeiters, die unter www.sally.io eingesehen werden kann. Der Auftragsverarbeiter verarbeitet Video- und Audioaufnahmen ausschließlich nach Weisung des Auftraggebers und hat keinen Zugriff auf die Inhalte. Die Aufnahmen werden verschlüsselt gespeichert und nur für die vereinbarte Dauer aufbewahrt. Eine Weitergabe an Dritte oder eigene Nutzung durch den Auftragsverarbeiter erfolgt nicht.

2. **Ort der Datenverarbeitung:**
   Die Verarbeitung und Speicherung personenbezogener Daten im Rahmen der Nutzung der KI erfolgt ausschließlich innerhalb der EU, vorzugsweise in Deutschland. Eine Übermittlung in Drittländer findet nicht statt.

3. **Keine Übermittlung in Drittländer:**
   Es erfolgt keine Übermittlung personenbezogener Daten in Drittländer. Sollte dies in Einzelfällen notwendig werden, erfolgt dies nur unter Einhaltung der entsprechenden DSGVO-Vorgaben und in Abstimmung mit dem Auftraggeber.

---

§ 9 Meldung von Datenschutzverletzungen *(Art. 33 und 34 DSGVO)*

1. **Meldepflicht des Auftragsverarbeiters:**
   Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten, die im Rahmen der Verarbeitung im Auftrag des Auftraggebers auftritt. Dies gilt insbesondere, wenn die

Datenschutzverletzung voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen könnte.

2. **Inhalt der Meldung:**
   Die Meldung muss folgende Informationen enthalten:
   - Eine Beschreibung der Art der Datenschutzverletzung,
   - Die Kategorien und die Anzahl der betroffenen personenbezogenen Daten sowie die Anzahl der betroffenen Personen,
   - Eine Beschreibung der vermuteten Ursachen der Datenschutzverletzung,
   - Die Maßnahmen zur Behebung der Verletzung sowie Maßnahmen zur Schadensminderung und Risikominimierung, die der Auftragsverarbeiter bereits ergriffen hat oder noch ergreifen wird,
   - Falls zutreffend, eine Empfehlung zur Benachrichtigung der betroffenen Personen, falls dies zur Wahrung der Rechte und Freiheiten der betroffenen Personen erforderlich ist.
3. **Zusammenarbeit bei der Meldung an die Aufsichtsbehörde:**
   Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Meldung der Datenschutzverletzung an die zuständige Aufsichtsbehörde, wenn dies erforderlich ist. Hierzu stellt der Auftragsverarbeiter alle notwendigen Informationen zur Verfügung, um sicherzustellen, dass der Auftraggeber seine Verpflichtungen gemäß Art. 33 DSGVO erfüllt.

---

§ 10 Löschung und Rückgabe der Daten *(Art. 28 Abs. 3 lit. g DSGVO)*

1. **Löschung und Rückgabe:**
   Nach Beendigung des Hauptvertrags, spätestens jedoch innerhalb von 30 Tagen nach Vertragsende, löscht der Auftragsverarbeiter sämtliche personenbezogene Daten, die im Rahmen der Auftragsverarbeitung verarbeitet wurden, oder gibt sie, nach Wahl des Auftraggebers, vollständig und in einem gängigen, maschinenlesbaren Format zurück. Dies gilt nicht für Daten, die der Auftragsverarbeiter aufgrund gesetzlicher Verpflichtungen aufbewahren muss.
2. **Bestätigung der Löschung:**
   Der Auftragsverarbeiter bestätigt dem Auftraggeber schriftlich, dass alle personenbezogenen Daten entweder gelöscht oder zurückgegeben wurden. Die Bestätigung erfolgt spätestens 30 Tage nach der Löschung oder Rückgabe.
3. **Ausnahmen:**
   Soweit der Auftragsverarbeiter nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, verpflichtet ist, personenbezogene Daten über

den Beendigungszeitpunkt des Vertrages hinaus aufzubewahren (z. B. für steuerrechtliche oder buchhalterische Zwecke), wird der Auftragsverarbeiter den Auftraggeber darüber informieren und sicherstellen, dass diese Daten gemäß den relevanten gesetzlichen Vorschriften gesperrt werden, sodass keine unbefugte Verarbeitung stattfindet.

---

§ 11 Haftung und Schadensersatz *(Art. 82 DSGVO)*

1. **Haftung des Auftragsverarbeiters:**
   Der Auftragsverarbeiter haftet für Schäden, die aufgrund einer nicht weisungsgemäßen Verarbeitung personenbezogener Daten entstanden sind, sofern der Auftragsverarbeiter gegen die Vorgaben der DSGVO oder die vertraglichen Vereinbarungen dieses Vertrages verstoßen hat. Dies umfasst insbesondere die unrechtmäßige Verarbeitung, den Verlust oder die unbefugte Offenlegung personenbezogener Daten.

2. **Haftung des Auftraggebers:**
   Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich und stellt sicher, dass die Verarbeitung auf einer gültigen Rechtsgrundlage gemäß Art. 6 DSGVO basiert. Der Auftraggeber haftet auch für die ordnungsgemäße Wahrung der Betroffenenrechte.

3. **Begrenzung der Haftung:**
   Die Haftung des Auftragsverarbeiters ist auf den direkten Schaden begrenzt, der durch die vertragliche Verletzung verursacht wurde. Eine Haftung für Folgeschäden, entgangenen Gewinn oder indirekte Schäden wird ausgeschlossen, es sei denn, der Schaden beruht auf Vorsatz oder grober Fahrlässigkeit des Auftragsverarbeiters.

4. **Schadensersatz:**
   Beide Parteien sind verpflichtet, sich gegenseitig unverzüglich über Schäden zu informieren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten entstehen. Die Parteien verpflichten sich zur Minderung des Schadens, soweit dies zumutbar ist. Schadensersatzansprüche können nur geltend gemacht werden, wenn die Partei, die den Schaden verursacht hat, ihre vertraglichen Pflichten oder die Vorgaben der DSGVO vorsätzlich oder grob fahrlässig verletzt hat.

5. **Mitwirkung des Auftraggebers:**
   Der Auftraggeber verpflichtet sich, alle erforderlichen Informationen bereitzustellen und mit dem Auftragsverarbeiter zusammenzuarbeiten, um im

Falle einer Schadensersatzforderung durch betroffene Personen oder Aufsichtsbehörden die Haftung zu klären und abzuwehren.

---

§ 12 Verbot der Vervielfältigung oder Weitergabe von Daten

1. **Verarbeitung der Daten:**
   Der Auftragsverarbeiter ist nicht berechtigt, personenbezogene Daten des Auftraggebers zu kopieren, zu vervielfältigen, zu speichern oder in sonstiger Weise zu verarbeiten, die nicht ausdrücklich durch diesen Vertrag oder die schriftliche Weisung des Auftraggebers gedeckt ist.

2. **Kein KI-Training mit Nutzerdaten:**
   Die vom Auftraggeber bereitgestellten und durch die Sally-App verarbeiteten Daten werden nicht zum Training von KI-Modellen verwendet. Eine Nutzung der Daten durch den Auftragsverarbeiter in eigener Verantwortung für eigene Geschäftszwecke ist ausgeschlossen. Dies gilt überdies auch für nicht-personenbezogene Daten.

3. **Unautorisierte Weitergabe:**
   Jegliche unautorisierte Weitergabe, Veräußern oder Nutzung der Daten, insbesondere zu eigenen Zwecken oder Zwecken Dritter, ist ausdrücklich untersagt.

4. **Folgen eines Verstoßes:**
   Im Falle eines Verstoßes gegen diese Bestimmungen ist der Auftraggeber berechtigt, den Vertrag fristlos zu kündigen und Schadensersatzansprüche geltend zu machen.

---

§ 13 Verzeichnis von Verarbeitungstätigkeiten

1. **Pflicht zur Führung eines Verarbeitungsverzeichnisses:**
   Der Auftragsverarbeiter verpflichtet sich, ein Verzeichnis der im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO zu führen. Dieses Verzeichnis umfasst alle wesentlichen Angaben zu den Verarbeitungsvorgängen, einschließlich der Zwecke der Verarbeitung, der Kategorien personenbezogener Daten und betroffener Personen sowie der technischen und organisatorischen Maßnahmen (TOMs).

2. **Verfügbarkeit des Verzeichnisses:**
   Der Auftragsverarbeiter stellt dem Auftraggeber auf dessen Anfrage eine Kopie oder Einsicht in das Verzeichnis der Verarbeitungstätigkeiten zur Verfügung, sofern dies für den Nachweis der Einhaltung der datenschutzrechtlichen Vorgaben erforderlich ist.

3. **Verpflichtungen des Auftraggebers:**
   Der Auftraggeber bleibt verpflichtet, ein eigenes Verzeichnis der von ihm durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO zu führen, welches die durch den Auftragsverarbeiter durchgeführten Verarbeitungstätigkeiten ebenfalls umfasst.

4. **Zusammenarbeit bei Prüfungen durch Aufsichtsbehörden:**
   Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung von Verpflichtungen gegenüber Aufsichtsbehörden, insbesondere durch die Bereitstellung von Informationen aus dem Verzeichnis der Verarbeitungstätigkeiten, sofern dies zur Einhaltung gesetzlicher Anforderungen erforderlich ist.

5. **Aktualisierungspflicht:**
   Der Auftragsverarbeiter verpflichtet sich, das Verzeichnis bei Änderungen oder Ergänzungen der Verarbeitungstätigkeiten unverzüglich zu aktualisieren und den Auftraggeber über wesentliche Änderungen zu informieren.

---

§ 14 Regelung im Insolvenzfall des Auftraggebers

1. **Meldepflicht des Auftraggebers:**
   Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter unverzüglich zu informieren, wenn ein Insolvenzverfahren über sein Vermögen beantragt oder eröffnet wird oder wenn vergleichbare Verfahren wie Zwangsvollstreckung, Pfändung oder Beschlagnahmung stattfinden.

2. **Fortsetzung der Verarbeitung im Insolvenzfall des Auftraggebers:**
   Im Falle der Insolvenz des Auftraggebers ist der Auftragsverarbeiter nicht verpflichtet, die vertraglich vereinbarte Verarbeitung personenbezogener Daten fortzusetzen, wenn dies aufgrund der Insolvenz des Auftraggebers nicht mehr möglich ist oder der Auftraggeber seine Verpflichtungen aus diesem Vertrag nicht mehr erfüllen kann. Der Auftragsverarbeiter hat jedoch weiterhin die Verpflichtung, personenbezogene Daten gemäß den geltenden Datenschutzvorschriften zu schützen.

3. **Rückgabe oder Löschung personenbezogener Daten im Insolvenzfall:**
   Im Falle der Insolvenz des Auftraggebers verpflichtet sich der Auftragsverarbeiter, alle personenbezogenen Daten, die im Rahmen der Auftragsverarbeitung verarbeitet wurden, unverzüglich an den Auftraggeber oder dessen Insolvenzverwalter zurückzugeben oder zu löschen, sofern dies gesetzlich zulässig ist. Ist die Rückgabe oder Löschung der Daten nicht möglich, ist der Auftragsverarbeiter verpflichtet, die Daten gemäß den vertraglichen Vereinbarungen weiterhin zu schützen.

4. **Kündigungsrecht des Auftragsverarbeiters:**
   Der Auftragsverarbeiter ist berechtigt, den Vertrag mit sofortiger Wirkung zu kündigen, wenn der Auftraggeber insolvent wird und dadurch die ordnungsgemäße Auftragsverarbeitung oder der Schutz personenbezogener Daten nicht mehr gewährleistet werden kann. In einem solchen Fall sind alle personenbezogenen Daten des Auftraggebers unverzüglich zurückzugeben oder zu löschen, sofern dies rechtlich zulässig ist.

---

§ 15 Geheimhaltungspflichten

1. **Verpflichtung zur Geheimhaltung:**
   Der Auftragsverarbeiter verpflichtet sich, sämtliche ihm im Rahmen dieses Vertragsverhältnisses bekanntwerdenden Informationen, einschließlich personenbezogener Daten und geschäftlicher Informationen des Auftraggebers, streng vertraulich zu behandeln.

2. **Zweckbindung:**
   Vertrauliche Informationen dürfen ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen verwendet werden. Eine Weitergabe an Dritte erfolgt nur nach vorheriger schriftlicher Zustimmung des Auftraggebers oder wenn dies gesetzlich erforderlich ist.

3. **Maßnahmen zum Schutz der Vertraulichkeit:**
   Der Auftragsverarbeiter verpflichtet sich, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Vertraulichkeit der ihm überlassenen Informationen jederzeit zu gewährleisten.

4. **Dauer der Geheimhaltungspflicht:**
   Die Verpflichtung zur Geheimhaltung besteht auch nach Beendigung des Vertragsverhältnisses unbefristet weiter.

5. **Ausnahmen:**
   Die Geheimhaltungspflichten gelten nicht für Informationen,
   a) die dem Auftragsverarbeiter vor ihrer Offenlegung nachweislich bekannt waren,
   b) die allgemein zugänglich oder bekannt sind, ohne dass dies auf einer Verletzung dieses Vertrags beruht, oder
   c) die aufgrund einer gesetzlichen Verpflichtung oder behördliche Anordnung offengelegt werden müssen.

---

§ 16 Verschwiegenheitspflicht nach § 203 StGB

1. **Aktivierungsbedingung**
   Dieser § 16 findet nur ergänzende Anwendung, sofern der Auftraggeber in Textform bestätigt, dass er Berufsgeheimnisträger im Sinne des § 203 StGB ist. Andernfalls gelten ausschließlich die allgemeinen Vertraulichkeitsregelungen des § 15 AVV.

2. **Anwendungsbereich / Berufsgeheimnisse**
   Soweit der Auftraggeber einer gesetzlichen Verschwiegenheitspflicht nach § 203 StGB unterliegt, erkennt der Auftragsverarbeiter an, dass ihm im Rahmen der Leistungserbringung Informationen zur Kenntnis gelangen können, die als Berufsgeheimnisse i. S. d. § 203 StGB geschützt sind (insbesondere solche nach § 43a BRAO i. V. m. BORA, § 57 StBerG, § 43 WPO, § 39a PAO; „Berufsgeheimnisse“).

3. **Übernahme der Verschwiegenheitspflicht / Grundsatz**
   Der Auftragsverarbeiter übernimmt die Verschwiegenheitspflicht des Auftraggebers gemäß § 203 StGB auf sich. Er wahrt über alle Berufsgeheimnisse, die ihm bei Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt werden, Stillschweigen, schützt diese vor unbefugtem Zugriff und verschafft sich nur insoweit Kenntnis, wie dies zur ordnungsgemäßen Vertragserfüllung erforderlich ist („Need-to-know“).

4. **Verpflichtung von Beschäftigten**
   Der Auftragsverarbeiter stellt sicher, dass alle Beschäftigten sowie etwaige Subunternehmer, die im Rahmen der Auftragsverarbeitung Zugriff auf Daten des Auftraggebers erhalten, ausdrücklich auf die Einhaltung der Verschwiegenheitspflicht gemäß § 203 StGB verpflichtet werden.

5. **Offenlegung nur bei gesetzlicher Pflicht**
   Eine Offenlegung von Berufsgeheimnissen erfolgt ausschließlich auf Weisung des Auftraggebers oder, sofern zwingendes Unionsrecht bzw. das Recht eines Mitgliedstaats dies verlangt. In diesem Fall informiert der Auftragsverarbeiter den Auftraggeber vorab über die rechtlichen Anforderungen, soweit dies rechtlich nicht untersagt ist, und beschränkt die Offenlegung auf das erforderliche Mindestmaß; entsprechende Zugriffe werden protokolliert.

6. **Dauer, Rückgabe, Löschung**
   Die Verschwiegenheitspflicht gilt zeitlich unbegrenzt und über das Vertragsende hinaus. Nach Vertragsende werden Unterlagen und Datenträger mit Berufsgeheimnissen nach Weisung des Auftraggebers sicher gelöscht; gesetzliche Aufbewahrungspflichten bleiben unberührt, in diesem Fall erfolgt eine Sperrung.

7. **Vorrang dieser Regelung**
   Diese Spezialregelung geht, soweit einschlägig, den allgemeinen Vertraulichkeitsverpflichtungen dieses Vertrages vor.

8. **Unberührt bleibende Pflichten**
   Weitergehende datenschutzrechtliche Verpflichtungen (insbesondere aus der DSGVO und dem AVV) bleiben von dieser Regelung unberührt.

---

§ 17 Kündigung des Vertrags

1. **Ordentliche Kündigung:**
   Der Vertrag, einschließlich des Abonnements, kann von beiden Parteien bis zu einem Tag vor Erneuerung des Abonnements gekündigt werden, sofern nichts anderes schriftlich vereinbart wurde.

2. **Außerordentliche Kündigung:**
   Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn:
   a) eine der Parteien wiederholt oder schwerwiegend gegen die vertraglichen oder gesetzlichen Pflichten verstößt, insbesondere in Bezug auf die Nutzung der bereitgestellten KI,
   b) über das Vermögen einer der Parteien ein Insolvenzverfahren eröffnet oder die Eröffnung eines solchen Verfahrens beantragt wird, oder
   c) durch Handlungen oder Unterlassungen einer Partei wodurch die Einhaltung der DSGVO oder anderer gesetzlicher Vorgaben nicht mehr gewährleistet werden kann.

3. **Ende des Abonnements:**
   Mit der Kündigung des Vertrags endet auch das Abonnement, und der Auftragsverarbeiter ist ab dem Kündigungszeitpunkt nicht mehr berechtigt, die bereitgestellten Daten oder die zur Verfügung gestellten Dienstleistungen zu nutzen, es sei denn, eine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

4. **Folgen der Kündigung:**
   a) Mit Beendigung des Vertragsverhältnisses verpflichtet sich der Auftragsverarbeiter, sämtliche im Rahmen der Verarbeitung und Nutzung der personenbezogenen Daten gesammelten Daten gemäß den datenschutzrechtlichen Anforderungen zu löschen, es sei denn, eine gesetzliche Verpflichtung zur weiteren Speicherung besteht.
   b) Der Auftragsverarbeiter hat die Löschung der Daten schriftlich zu bestätigen.

---

§ 18 Gerichtsstand und anwendbares Recht

1. **Anwendbares Recht:**
   Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des internationalen Privatrechts und des UN-Kaufrechts.

2. **Gerichtsstand:**
   Für alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag ergeben, wird als ausschließlicher Gerichtsstand der Sitz des Auftragsverarbeiters vereinbart (Mannheim), sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

---

§ 19 Salvatorische Klausel

1. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

2. Anstelle der unwirksamen oder undurchführbaren Bestimmung gilt diejenige Regelung, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

3. Dasselbe gilt im Falle von Regelungslücken.

Anlagen

1. Technische und organisatorische Maßnahmen (Anlage 1)
2. Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters (Anlage 2)
3. Eingesetzte Subunternehmer (Anlage 3)
4. Datenschutz-Folgenabschätzung (DSFA) für die KI-Lösung (Anlage 4)
5. KI-Konformitätserklärung nach EU AI Act (Anlage 5)
6. Einhaltung der Verordnung (EU) 2024/1689 AI Act (Anlage 6)
7. Prozessdarstellungen zur Nutzung von Sally (Anlage 7)

Unterschriften

Ort, Datum:

Julian Kissel

Auftragsverarbeiter
Julian Kissel
CEO

Auftraggeber
Name
Position (vertretungsberechtigt)

Anlage 1: Technische und organisatorische Maßnahmen

1. Zugangskontrolle (Hosting-Standort)
Die physische Zugangskontrolle wird durch unsere Cloud-Hosting-Dienstleister in der EU (Microsoft Azure) und in Deutschland (Hetzner - stark bevorzugt) sichergestellt. Diese sind verpflichtet, Rechenzentren mit hohen Sicherheitsstandards zu betreiben (z. B. ISO 27001) und vor unbefugtem Zugang zu schützen.

2. Zugriffskontrolle (logisch)
Der Zugang zur KI-Anwendung wird durch folgende Maßnahmen gesichert:

- Authentifizierung: Kunden (Auftraggeber) laden die KI in ihre Meetings über registrierte Konten ein. Unautorisierte Zugriffe sind ausgeschlossen.
- Verschlüsselung: Die Übertragung aller Daten erfolgt ausschließlich über verschlüsselte Kanäle (z. B. HTTPS).
- Zugriffsprotokollierung: Alle Anfragen werden protokolliert und auf mögliche Missbrauchsmuster hin überwacht.
- Zugriff auf gespeicherte Videoaufnahmen erfolgt nur durch berechtigte Nutzer gemäß Berechtigungskonzept.
- Gespeicherte Videos sind verschlüsselt und können nur durch autorisierte Instanzen entschlüsselt werden.
- Alle Arbeitsplatzrechner sind zentral über Microsoft Intune verwaltet, wodurch Sicherheitsrichtlinien und Gerätekonfigurationen einheitlich umgesetzt werden.
- Zusätzlich ist Microsoft Defender for Endpoint auf allen Geräten aktiv, um erweiterte Bedrohungserkennung und -abwehr zu gewährleisten.
- Microsoft Defender Antivirus ist auf allen Endgeräten installiert und durchgehend aktiviert.

3. Weitergabekontrolle
Maßnahmen zur Sicherstellung der geschützten Übertragung und Speicherung von Daten:

- Verschlüsselung von Datenübertragungen mit TLS 1.3/SSL.
- Sicherstellung der Protokollierung bei Datenweitergaben.
- Übermittlung personenbezogener Daten an Dritte nur mit vorheriger Zustimmung des Auftraggebers.
- Einsatz von VPNs für sichere Remote-Verbindungen.
- Keine Weitergabe von Videoaufzeichnungen an Dritte ohne explizite Anweisung des Auftraggebers.

- Verarbeitung der Videoaufnahmen erfolgt ausschließlich innerhalb der vorgesehenen Systeme.

4. Eingabekontrolle
Maßnahmen zur Nachvollziehbarkeit der Verarbeitung personenbezogener Daten:

- Protokollierung aller Eingaben, Änderungen und Löschungen von personenbezogenen Daten.
- Dokumentation von Nutzeraktivitäten in Audit-Logs.
- Schulung der Mitarbeiter zur ordnungsgemäßen Datenverarbeitung.
- Dokumentation von Zugriffen auf gespeicherte Videoaufnahmen.
- Transparente Kennzeichnung der Verarbeitung von Videodaten in Systemprotokollen.

5. Auftragskontrolle
Maßnahmen zur Sicherstellung der weisungsgemäßen Datenverarbeitung:

- Verarbeitungen erfolgen ausschließlich gemäß den Weisungen des Auftraggebers (Art. 28 DSGVO).
- Schulung der Mitarbeiter zu den Weisungen und der DSGVO.
- Regelmäßige Überprüfung der Einhaltung durch interne Audits.
- Nutzung der Videoaufnahmen ausschließlich für die Transkription, keine Speicherung über die vereinbarten Fristen hinaus.

6. Verfügbarkeitskontrolle
Maßnahmen zur Sicherung der Verfügbarkeit und des Schutzes vor Datenverlust:

- Regelmäßige Backups der Systeme (mindestens täglich).
- Einsatz redundanter Systeme (z. B. RAID-Verbunde, Failover-Lösungen).
- Notfallpläne und regelmäßige Tests von Wiederherstellungsmaßnahmen.
- Sicherstellung, dass Video- und sonstige Aufnahmen in keiner Form verfügbar sind, nachdem der Auftraggeber die Löschung dieser Daten veranlasst hat

7. Umgang mit temporären Rohdaten (Audio-/Videoaufnahmen):

- Rohdaten, die ausschließlich zur Durchführung der Transkription und Analyse verarbeitet werden, werden nach Abschluss des jeweiligen Verarbeitungsvorgangs automatisch gelöscht.
- Eine Speicherung von Rohdaten über den Verarbeitungszeitpunkt hinaus erfolgt nicht, es sei denn, der Auftraggeber hat die Speicherung der Aufnahme ausdrücklich gewünscht.

- Kundenseitig gespeicherte Audio- und Videodaten werden ausschließlich nach Weisung des Auftraggebers gelöscht oder nach Vertragsende gemäß § 10 AVV.

8. Trennungsgebot

Maßnahmen zur getrennten Verarbeitung von Daten für unterschiedliche Auftraggeber:

- Logische Trennung der Daten durch unterschiedliche Datenbanken oder Verzeichnisse.
- Zugriffsbeschränkungen basierend auf den Mandantenrechten.
- Strikte Trennung von Entwicklungs- und Produktionssystemen.
- Videoaufnahmen werden mandantengetrennt gespeichert und verarbeitet.

9. Verschlüsselung

Maßnahmen zur Sicherstellung der Vertraulichkeit der Daten:

- Verschlüsselung gespeicherter Daten mit AES-256.
- Nutzung moderner Verschlüsselungsstandards für Datenübertragungen (z. B. HTTPS).
- Verschlüsselung mobiler Datenträger (z. B. USB-Sticks, Laptops).
- Videoaufzeichnungen werden verschlüsselt gespeichert (AES-256).
- Zugriff auf verschlüsselte Daten erfolgt nur durch dedizierte, autorisierte Instanzen.

10. Maßnahmen bei Störungen und Datenschutzverletzungen

- Einrichtung eines Prozesses zur Meldung und Bearbeitung von Datenschutzvorfällen (Incident Management).
- Unverzügliche Benachrichtigung des Auftraggebers im Fall von Datenpannen gemäß Art. 33 DSGVO.
- Dokumentation von Sicherheitsvorfällen und ergriffenen Maßnahmen.

11. Sensibilisierung und Schulung von Mitarbeitern

- Regelmäßige Schulungen zum Datenschutz und zur Informationssicherheit.
- Vertraulichkeitsverpflichtung aller Mitarbeiter, die Zugriff auf personenbezogene Daten haben.
- Prüfung und Überwachung der Einhaltung von Sicherheitsrichtlinien durch die Mitarbeiter.
- Meldung eines Vorfalls auch, wenn es sich um unbefugten Zugriff oder eine unrechtmäßige Nutzung von Videoaufnahmen handelt.

Diese Maßnahmen werden regelmäßig überprüft und an den Stand der Technik sowie an die Anforderungen des Auftraggebers angepasst. Änderungen oder Ergänzungen dieser Anlage werden schriftlich vereinbart.

Anlage 2: Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters *(Art. 30 Abs. 2 DSGVO)*

Nr.	Verarbeitungstätigkeit	Zweck der Verarbeitung	Kategorien betroffener Personen	Kategorien personenbezogener Daten	Rechtsgrundlage	Empfänger (falls zutreffend)	Löschfristen	Drittlandübermittlung (ja/nein)
1	Transkription und Protokollierung von Meetings	Bereitstellung von Meeting-Transkripten und -Protokollen	Meeting-Teilnehmer (z. B. Kunden, Geschäftspartner, Mitarbeiter des Auftraggebers)	Video- und Audioaufnahmen, Transkriptionen, Metadaten (Teilnehmer, Zeit, Dauer)	Art. 6 DSGVO (Auftragsverarbeitung)	Keine	30 Tage nach Vertragsende oder Weisung des Auftraggebers	Nein

Zusatzinformationen

- **TOMs (Technische und Organisatorische Maßnahmen):** Siehe Anlage 1
- **Datenschutzbeauftragter:**
  - Name: Norton Engele
  - E-Mail-Adresse: datenschutz@sally.io

Anlage 3: Eingesetzte Subunternehmer

Name des Subunternehmers	Serverstandort / Sitz	Erbrachte Dienstleistung	Unbefristeter Vertrag & Datenverarbeitung innerhalb der EU	Datenschutzerklärung
Hetzner Online GmbH	Serverstandort: Deutschland Sitz: Industriestr. 25, 91710 Gunzenhausen, Deutschland	Cloud-Infrastruktur / Webhosting / Backups	Ja EU – Deutschland	Hetzner Datenschutzerklärung
Microsoft Ireland Operations Limited	Serverstandort: Niederlande Sitz: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland.	Cloud-Infrastruktur für Rechenleistung und Speicherung	Ja EU – Niederlande	Microsoft Datenschutzerklärung
Amazon Web Services EMEA SARL (AWS)	Serverstandort: Deutschland / Irland	Video- / Audiodistribution	Ja EU – Deutschland / Irland	AWS Datenschutzerklärung

	Sitz: 38 Avenue John F. Kennedy, L-1855 Luxembourg			
DeepL SE	Serverstandort: Deutschland Sitz: Maarweg 165, 50825 Köln, Deutschland.	KI-gestützte Übersetzungen	Ja EU – Deutschland	DeepL Datenschutzerklärung
Stripe Payments Europe, Limited	Serverstandort: Irland Sitz: The One Building, 1 Lower Grand Canal Street, Dublin 2, D02 HD59, Ireland	Zahlungsabwicklung und Transaktionsverarbeitung	Ja EU – Irland	Stripe Datenschutzerklärung
Strato AG	Serverstandort: Deutschland Sitz: Pascalstraße 10, 10587 Berlin, Deutschland	Webhosting und Infrastruktur	Ja EU – Deutschland	Strato Datenschutzerklärung

Azure OpenAI (Microsoft Ireland Operations Limited)	Serverstandort: Schweden Sitz: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland.	KI-Dienste von OpenAI (bereitgestellt über Microsoft Azure)	Ja EU – Schweden	Microsoft Datenschutzerklärung

Anlage 4: Datenschutz-Folgenabschätzung (DSFA) für die KI-Lösung

1. Einleitung

Diese Datenschutz-Folgenabschätzung (DSFA) erfolgt gemäß Art. 35 DSGVO für die KI-gestützte Meeting-Dokumentationssoftware des Unternehmens. Ziel ist die systematische Analyse der Risiken für betroffene Personen sowie die Festlegung geeigneter Schutzmaßnahmen.

2. Beschreibung der Verarbeitung

- **Zweck der Verarbeitung:**
  Automatische Transkription, Analyse und Zusammenfassung von Meetings zur effizienten Dokumentation und Nachverfolgung.
- **Verarbeitete personenbezogene Daten:**
  - Gesprochene Sprache (Transkripte)
  - Namen und Kontaktdaten der Meeting-Teilnehmer (soweit erfasst)
  - Metadaten (Datum, Uhrzeit, Dauer, Meeting-ID)
  - Videoaufzeichnungen der Meetings zur Unterstützung der Transkription
- Betroffene Personen: Teilnehmer von Meetings (Kunden, Partner, Mitarbeiter).
- Datenquellen: Live-Audio- und Videoaufnahmen aus Online-Meetings.
- Auftragsverarbeiter: Microsoft Azure (Hosting), Azure OpenAI (Textanalyse)

3. Bewertung der Notwendigkeit und Verhältnismäßigkeit

- Die Verarbeitung erfolgt, um eine effiziente Meeting-Dokumentation bereitzustellen und manuelle Notizen zu ersetzen.
- Die Verhältnismäßigkeit ist gewahrt, da nur relevante Daten verarbeitet werden.
- Die Verarbeitung basiert auf der Einwilligung der Teilnehmer oder auf berechtigtem Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO.

4. Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen
Potenzielle Risiken:

- Unbefugter Zugriff auf Transkripte, Videoaufnahmen und Metadaten.
- Missbrauch oder Fehlinterpretation der Daten.
- Unzureichende Transparenz für die betroffenen Personen.
- Risiken durch den Einsatz externer KI-Dienstleister.

5. Maßnahmen zur Risikominderung

- **Technische und organisatorische Maßnahmen (TOMs):**
    - Verschlüsselung von Transkripten, Videoaufnahmen und gespeicherten Daten.
    - Zugriffsbeschränkungen und rollenbasierte Berechtigungen.
    - Für Benutzer aus der Europäischen Union (EU) bleibt der gesamte Datenverkehr vollständig innerhalb der EU-Datengrenze. Es erfolgt keinerlei Übertragung oder Verarbeitung personenbezogener Daten außerhalb der Europäischen Union.
    - Pseudonymisierung sensibler Daten.
    - Sicherstellung, dass Video- und sonstige Aufnahmen in keiner Form verfügbar sind, nachdem der Auftraggeber die Löschung dieser Daten veranlasst hat
    - Transparente Information der Nutzer über die Aufzeichnung und Verarbeitung von Video.
    - Regelmäßige Datenschutz- und Sicherheitsprüfungen.
    - Weitere detaillierte Maßnahmen siehe Anlage 1: Technische und organisatorische Maßnahmen.
- **Konkretisierung der Löschfristen für Rohdaten:**

- Temporäre Rohdaten, die zur Transkription und Analyse benötigt werden, werden unmittelbar nach Abschluss der Verarbeitung gelöscht.
- Eine dauerhafte Speicherung von Rohdaten erfolgt ausschließlich auf ausdrücklichen Wunsch des Auftraggebers.
- Im Übrigen gilt die Löschregelung des AVV (§ 10).
- Vertragsrechtliche Absicherungen:
- Abschluss von Auftragsverarbeitungsverträgen (AVV) mit allen Subdienstleistern.
- Sicherstellung der DSGVO-Konformität externer Dienstleister.

- **Betroffenenrechte:**
  - Transparente Information über die Datenverarbeitung.
  - Implementierung von Löschfristen und Widerspruchsrechten.

6. Fazit

Nach der Bewertung der Risiken und implementierten Maßnahmen wird die Verarbeitung als DSGVO-konform und mit vertretbarem Risiko für die betroffenen Personen eingestuft. Die Datenschutz-Folgenabschätzung wird regelmäßig überprüft und aktualisiert.

Anlage 5: KI-Konformitätserklärung nach EU AI Act

1. Einleitung Diese Erklärung erfolgt gemäß der Verordnung (EU) 2024/1689 (AI Act) und beschreibt die Konformität der KI-gestützten Meeting-Dokumentationssoftware mit den Anforderungen der Verordnung. Ziel ist die Transparenz über die eingesetzten KI-Technologien und deren Auswirkungen auf die betroffenen Personen.

2. Beschreibung des KI-Systems

- **Funktion:** Automatische Transkription, Zusammenfassung und Analyse gesprochener Inhalte in Meetings.
- **Datenverarbeitung:** Sprache und Videoaufzeichnungen zur besseren Transkription.
- **Verarbeitungszweck:** Dokumentation und Nachverfolgung von Meeting-Inhalten.
- **Eingesetzte KI-Technologien:** Spracherkennung und Textanalyse durch spezialisierte Modelle.

3. Einstufung nach dem AI Act Das System wird nicht als Hochrisiko-KI gemäß Anhang III der Verordnung (EU) 2024/1689 eingestuft, da es keine biometrische Identifizierung, Verhaltensanalyse oder automatisierte Entscheidungsfindung mit wesentlichen Auswirkungen auf die betroffenen Personen durchführt. Die Videoaufzeichnung dient ausschließlich zur Unterstützung der Transkription und wird nicht zur Analyse von Gesichtsausdrücken, Emotionen oder Verhalten genutzt.

4. Maßnahmen zur Einhaltung der Verordnung

- **Transparenz:** Nutzer werden über den Einsatz der KI und ihre Funktionsweise informiert.
- **Datenschutz & Sicherheit:** Verarbeitung ausschließlich innerhalb der EU, verschlüsselte Speicherung, Zugriffsbeschränkungen und regelmäßige Prüfungen (siehe Anlage 1: Technische und organisatorische Maßnahmen).
- **Vertragliche Absicherungen:** Auftragsverarbeitungsverträge (AVV) mit Subdienstleistern gemäß DSGVO.
- **Einschränkungen der Nutzung:** Keine Nutzung von Daten zur Verbesserung oder zum Training von KI-Modellen.

5. Fazit Das KI-System erfüllt die Anforderungen des AI Act und stellt keine Hochrisiko-Anwendung dar. Die eingesetzten Maßnahmen gewährleisten Datenschutz, Transparenz und Sicherheit für betroffene Personen. Diese Erklärung wird regelmäßig überprüft und aktualisiert, um der weiteren Entwicklung regulatorischer Anforderungen zu entsprechen.

Anlage 6: Einhaltung der Verordnung (EU) 2024/1689 (AI Act)

1. **Risikomanagement und Compliance**
   Der Auftragsverarbeiter verpflichtet sich, die Vorgaben der Verordnung (EU) 2024/1689 (AI Act) einzuhalten. Dies umfasst insbesondere die Durchführung einer Risikobewertung des KI-Systems gemäß den Anforderungen der Verordnung sowie die Implementierung von geeigneten Maßnahmen zur Risikominderung.

2. **Transparenz und Nachvollziehbarkeit**
   Der Auftragsverarbeiter stellt sicher, dass das KI-System so konzipiert ist, dass Entscheidungen, die Auswirkungen auf betroffene Personen haben, nachvollziehbar und dokumentiert sind. Die Dokumentation zur Funktionsweise der KI wird auf Anfrage zur Verfügung gestellt, soweit keine Geschäftsgeheimnisse oder Schutzrechte entgegenstehen.

3. **Sicherheit und Robustheit**
   Der Auftragsverarbeiter gewährleistet, dass das KI-System technischen und organisatorischen Sicherheitsmaßnahmen unterliegt, um Fehlfunktionen, unbefugte Zugriffe und Manipulationen zu verhindern. Diese Maßnahmen sind in **Anlage 1: Technische und organisatorische Maßnahmen** näher beschrieben.

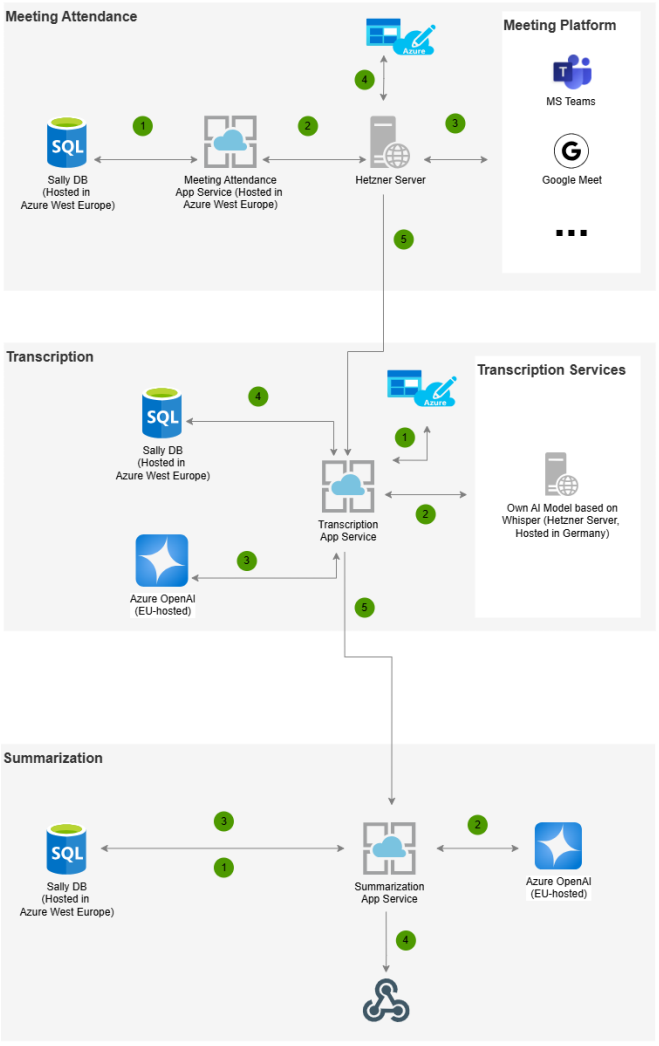
4. **Nicht-Diskriminierung und Fairness**
   Der Auftragsverarbeiter trifft angemessene Maßnahmen zur Vermeidung systematischer Verzerrungen (Bias) im KI-Modell, die zu Diskriminierungen führen könnten. Dies umfasst regelmäßige Prüfungen der Trainingsdaten und der Modellentscheidungen.

5. **Laufende Überwachung und Berichterstattung**
   Der Auftragsverarbeiter überprüft das KI-System regelmäßig auf die Einhaltung der Verordnung (EU) 2024/1689 und dokumentiert relevante Prüfungen und Erkenntnisse. Wesentliche Änderungen am KI-System oder neu erkannte Risiken werden dem Verantwortlichen unverzüglich mitgeteilt.

6. **Zusammenarbeit mit dem Verantwortlichen**
   Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Verpflichtungen aus der Verordnung (EU) 2024/1689, insbesondere im Hinblick auf Anfragen von Aufsichtsbehörden oder betroffenen Personen.

7. **Verweise auf bestehende Dokumentation**
   Ergänzende Regelungen zur Datenverarbeitung, Sicherheit und Verantwortlichkeiten sind bereits in folgenden Anlagen enthalten:

Anlage 7: Prozessdarstellungen zur Nutzung von Sally

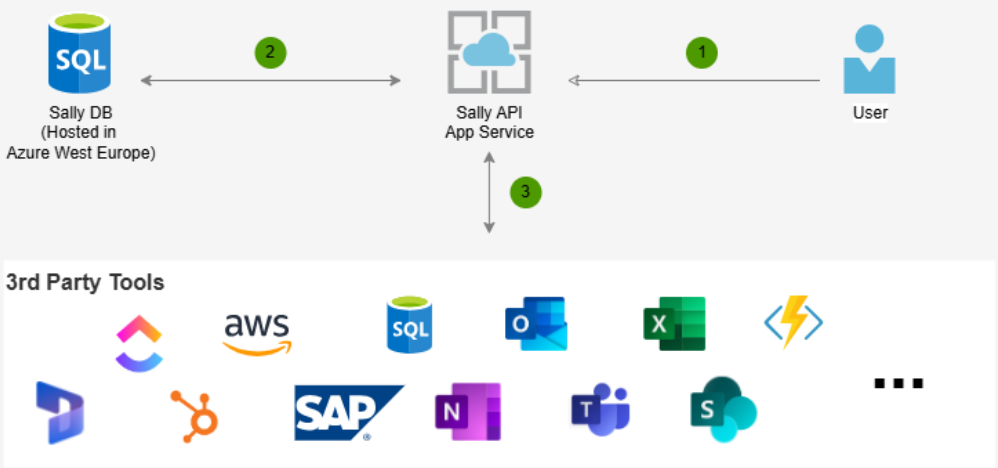


1. The Meeting Attendance Service uses the Sally DB data to check whether attendance at a meeting is expected. Both systems are hosted in Azure in the 'West Europe' data centre.
2. If a meeting has been found that Sally should attend, a new Hetzner node is started in our Kubernetes cluster and the meeting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

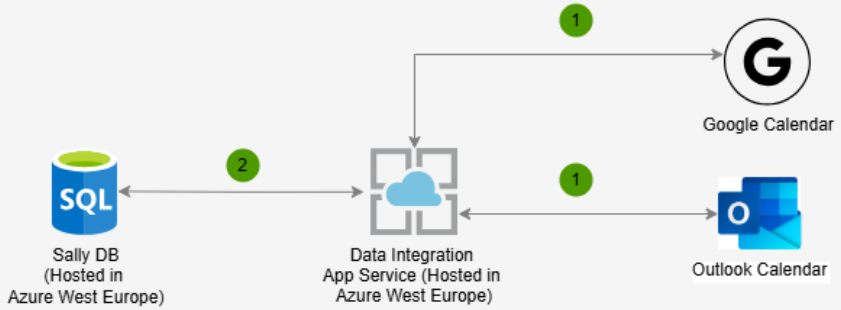
1. Based on the HTTPS request, the Summarisation Service, which is hosted within the EU (Azure data centre: West Europe), loads from the Sally DB via encrypted connection the information from the transcription and also all additional data known for the appointment (subject, description, participant,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