Security und Data Privacy Whitepaper

für Summie.ai, betrieben von der Solid Rock Ventures UG

15. Januar 2024 — Version 1.0

Einleitung

Im Zeitalter der Digitalisierung ist die Sicherheit privater Daten von entscheidender Bedeutung. Für Summie.ai, eine mobile Applikation, die Audiodaten für Transkription und Zusammenfassung verarbeitet, steht der Schutz dieser sensiblen Informationen an erster Stelle. Dieses Whitepaper hebt die umfangreichen Maßnahmen hervor, die wir implementiert haben, um die Privatsphäre und Sicherheit unserer Nutzer zu gewährleisten.

Auswahl der Dienstleister

Bei der Auswahl unserer externen Dienstleister gehen wir äußerst sorgfältig vor, um sowohl sicherheitsrelevante als auch eine geschlossene Kette von höchsten Datenschutzstandards gewährleisten zu können. Mit allen beteiligten Unternehmen, einschließlich OpenAI (OpenAI Ireland Ltd.) für die Verarbeitung von Audiodaten, haben wir einen Data Processing Agreement (DPA) unterzeichnet. Dies stellt sicher, dass alle Partner die von der EU geforderten Standards für Datenschutz und Datensicherheit einhalten.

Datenspeicherung

Unsere Dateninfrastruktur basiert auf der AWS Amazon Cloud in Frankfurt, Deutschland. Hierbei werden ausschließlich Server in Deutschland genutzt, um die Speicherung von personenbezogenen Informationen (PII) gemäß EU-DSGVO zu gewährleisten. Nutzerdaten werden auf nicht-öffentlichen Langzeitspeichern wie Amazon S3 und DynamoDB sicher verwahrt.

Zertifizierungen des AWS Data Centers

AWS bietet für diese Speicherklassen umfassende Sicherheitsstandards und Compliance-Zertifizierungen, darunter SEC Rule 17a-4, PCI-DSS, HIPAA/HITECH, FedRAMP, EU-DSGVO und FISMA. Das AWS Data Center in Frankfurt ist zudem nach ISO 27001, SOC2 Type 2 und GDPR konform zertifiziert, was unsere Verpflichtung zu höchsten Sicherheitsstandards unterstreicht.

Datentransfer zu OpenAI

Daten, die an OpenAI in den USA übermittelt werden, sind durch TLS-Verschlüsselung geschützt. OpenAI verpflichtet sich, gemäß den Bedingungen im DPA und den Terms of Service, diese Daten weder zu speichern noch weiterzuverarbeiten, einschließlich der Nichtnutzung für Trainingszwecke.

Datenaufbewahrung

Audiodaten werden lediglich für einen Zeitraum von 7 Tagen gespeichert und dienen ausschließlich Supportzwecken. Diese Daten verbleiben für diese Zeit auf unseren AWS Servern in Frankfurt und dem jeweiligen Endgerät des Nutzers.

Passwortsicherheit

Passwörter unserer Nutzer werden verschlüsselt gespeichert. Wir erzwingen die Erstellung sicherer Passwörter durch Vorgaben bezüglich der Länge, Nutzung von Sonderzeichen sowie Groß- und Kleinschreibung.

Sicherer Datentransfer

Die Übertragung von Daten erfolgt stets über TLS-gesicherte Endpunkte via Webhook an unsere AWS Server, um eine sichere Datenübermittlung zu gewährleisten.

Softwareentwicklung und Updates

Alle Updates durchlaufen vor der Implementierung in die Produktivumgebung eine sorgfältige Überprüfung und Tests nach dem 4-Augen-Prinzip. Dies stellt sicher, dass alle neuen Features den höchsten Sicherheitsstandards entsprechen.

Verarbeitung von PII

Die Verarbeitung von personenbezogenen Daten erfolgt strikt getrennt von Entwicklungssystemen. Kundendaten werden separat von PII behandelt und in unterschiedlichen Datenbanktabellen gespeichert. Nutzer haben zudem die Möglichkeit, einen verschlüsselten Dump ihrer PII zu beantragen.

Security & Privacy Roadmap

Im letzten Abschnitt dieses Whitepapers möchten wir auf unsere Privacy Roadmap eingehen. Eines unserer zentralen Ziele in 2024 ist es, die Modelle GPT (LLM, genutzt für verschiedene Zusammenfassungen und Meeting Analysen) und Whisper (KI-basierter Speech-to-Text Service) von OpenAI in der Microsoft Azure Cloud auf europäischen Servern zu hosten. Diese Maßnahme wird dazu beitragen, dass keine Datenübertragung in die USA mehr erforderlich ist, wodurch der Bedarf an einem DPA (Data Processing Agreement) und einer TIA (Transatlantic Impact Assessment) entfällt. Dies ist ein wesentlicher Schritt, um die Einhaltung der EU-Datenschutzstandards weiter zu stärken und die Privatsphäre unserer Nutzer noch besser zu schützen.

Zusammenfassend setzt Summie.ai auf eine Kombination aus strengen Sicherheitsprotokollen, sorgfältiger Auswahl von Dienstleistern und ständiger Überwachung und Verbesserung unserer Datenschutzpraktiken. Unser Engagement für den Schutz der Privatsphäre und Sicherheit unserer Nutzer steht im Mittelpunkt unserer Unternehmensphilosophie und treibt unsere kontinuierlichen Bemühungen in diesem Bereich voran.

Dokumentation (Annex 1-6)

Im Anhang dieses Whitepapers finden Sie wichtige Dokumente, darunter:

Annex 1 – Security Infrastructure Diagramm

Annex 2 – DPA mit OpenAI Ireland Ltd.

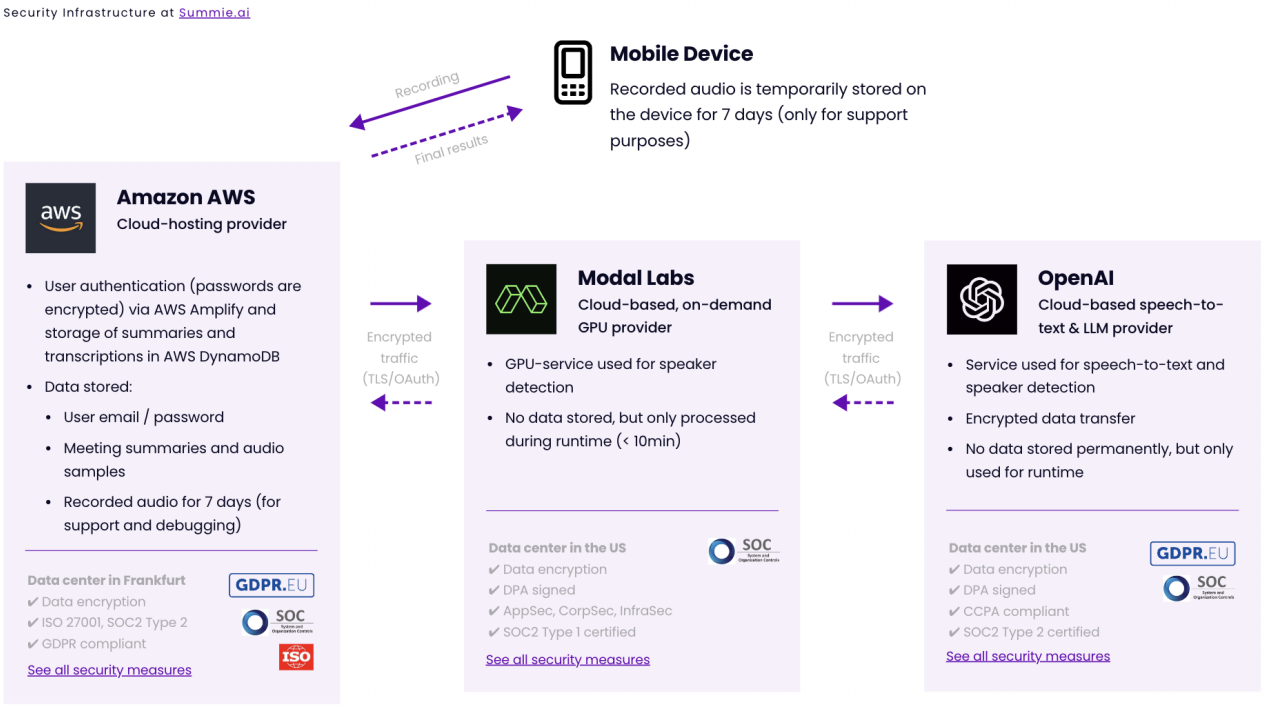
Annex 3 – DPA mit Modal Labs Inc.

Annex 4 – Technisch Organisatorischen Maßnahmen (TOM)

Annex 5 – Datenschutzhinweise nach Artikel 13 & 14 DSGVO

Annex 6 – Links zu den Terms of Service, Privacy Policy und GDPR-relevanten Dokumenten von Summie.ai und den genutzten Drittanbietern.

Annex 1 – Security Infrastructure Diagramm



Annex 2 – DPA mit OpenAI Ireland Ltd.

Das gesamte DPA (Data Processing Agreement) mit OpenAI Ireland Ltd. kann hier eingesehen und heruntergeladen werden.

Einen Auszug der relevanten EU-Standardvertragsklauseln (EU SCCs) finden Sie nachfolgend.

7. **Standard Contractual Clauses**.
   a. OpenAI will process Customer Data that originates in the European Economic Area in accordance with the standard contractual clauses adopted by the EU Commission on June 4, 2021 ("**EU SCCs**") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
      i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and OpenAI is processing Customer Data as a processor.
      ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and OpenAI is processing Customer Data as a sub-processor.
   b. For each module of the EU SCCs, where applicable, the following applies:
      i. The optional docking clause in Clause 7 does not apply;
      ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.
      iii. In Clause 11, the optional language does not apply;
      iv. All square brackets in Clause 13 are hereby removed;
      v. In Clause 17 (Option 1), the EU SCCs will be governed by the EU member state where the data exporter is located;
      vi. In Clause 18(b), disputes will be resolved before the courts of the EU member state where the data exporter is located;
      vii. Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs;
      viii. Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and
   c. Customer Data originating from Switzerland shall be processed in accordance with the EU SCCs with the following amendments:
      i. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.
      ii. "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023.
      iii. The term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
      iv. The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.
      v. The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP

Annex 3 – DPA mit Modal Labs Inc.

Das gesamte DPA (Data Processing Agreement) mit OpenAI Ireland Ltd. kann hier eingesehen und heruntergeladen werden.

Annex 4 – Technisch Organisatorischen Maßnahmen (TOM)

Die TOM können hier eingesehen und heruntergeladen werden.
Einen Auszug finden Sie nachfolgend.

Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO, 2024 Solid Rock Ventures UG
(Betreiber von Summie.ai)

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Kontrolle der Weitergabe
5. Kontrolle des Auftragsverarbeiters
6. Verfügbarkeitskontrolle
7. Trennungsgebot
8. Organisationskontrolle

1 — Zutrittskontrolle

Entfällt, da der Zugang zu unseren Systemen nicht ortsabhängig erfolgt. Alle Mitarbeiter können sich auch remote anmelden (siehe Sicherheitsvorkehrungen in Abschnitt 2).

2 — Zugangskontrolle

Wir betreiben unsere Systeme mit Amazon Web Services (AWS). Dabei existieren innerhalb unserer AWS Organisation hermetisch gegeneinander abgetrennte Nutzerkonten für a) den produktiven Betrieb unserer Software, b) die Staging-Umgebung und c) pro Mitarbeiter/Entwickler. Die produktive Umgebung unseres Clouddienstes ist durch den Geschäftsführer und die Entwickler zugänglich und mit einem Multifaktor-Anmeldeverfahren gesichert, in dieser personenbezogene Daten (personally identifiable information, PII) liegen.

3 — Zugriffskontrolle

Kundenseitig erfolgt der Zugang durch eine Anmeldung über den Amazon AWS Service Cognito/Amplify, in dem Passwörter verschlüsselt abgelegt werden. Es ist keine Authentifizierung mit einem Hardware-Device oder per Multifaktor-Authentifizierung (MFA) notwendig. Einen Zugang zu den erhobenen PII über eine dem Kunden zugängliche Oberfläche gibt es derzeit nicht. Die Daten werden über einen TLS-gesicherten Endpunkt via Webhook an die AWS Services übertragen.

4 — Kontrolle der Weitergabe

Wir erzwingen vom Nutzer das Erstellen sicherer Passwörter durch Erstellungsregeln für bestimmte Passwortlänge, sowie das Nutzen von Sonderzeichen und Groß- und Kleinschreibung. Es kann ein verschlüsselter Dump der PII durch den Nutzer angefordert werden.

5 — Kontrolle des Auftragsverarbeiters

Wir beschäftigen in Deutschland und Mazedonien ansässige Software-Entwickler auf Vertragsbasis. Abgesehen von unserem Leiter der Technik haben die Entwickler keinen Zugriff auf die erhobenen PII. Wir beschäftigen keine Subunternehmen, und abgesehen von Amazon/AWS, Modal Labs Inc. und OpenAI Inc. gibt es keine dritten technischen Dienstleister, durch deren Systeme von uns erhobene PII fließen. Für die Speicherung von PII nutzen wir ausschließlich Server mit Standort innerhalb der EU (AWS Europe/Frankfurt).

6 — Verfügbarkeitskontrolle

Nutzerdaten werden sämtlich auf einen nicht-öffentlichen Langzeit-Speicher abgelegt (S3 bzw. DynamoDB) und können dort granular eingesehen oder gelöscht werden. AWS gewährleistet für diese Speicherklassen umfangreiche Sicherheitsstandards und Compliance-Zertifizierungen, darunter SEC Rule 17a-4, PCI-DSS, HIPAA/HITECH, FedRAMP, EU-DSGVO und FISMA.

7 — Trennungsgebot

Die Verarbeitung von PII erfolgt getrennt von Entwicklungssystemen, unsere Kundendaten werden separat von PII verarbeitet und in separaten Tabellen vorgehalten.

8 — Organisationskontrolle

Audits unserer Logs- und Zugriffe finden zyklisch statt. So minimieren wir das Risiko offener Endpunkte oder Schnittstellen — auch wenn über diese keinesfalls PII zugreifbar sind (siehe oben). Bevor Updates in die Produktivumgebung ausgerollt werden, wird der betreffende Quellcode nach dem 4-Augen-Prinzip geprüft und getestet.

Annex 5 – Datenschutzhinweise nach Artikel 13 & 14 DSGVO

Die entsprechenden Informationen nach Art. 13 DSGVO / Datenschutzerklärung können hier eingesehen und heruntergeladen werden.

Annex 6 – Links

Summie	https://www.summie.ai/terms	Terms of Use
	https://www.summie.ai/privacy	Privacy Policy
AWS Amazon	https://aws.amazon.com/de/compliance/gdpr-center/	Amazon AWS DSGVO Zentrum
OpenAI Ireland Ltd.	https://trust.openai.com/	Security & Privacy Portal zu Sicherheits- und Privacybezogenen Maßnahmen, inkl. DSGVO, Pentest, sowie SOC 2 und SOC 3 Reports
	https://openai.com/policies/business-terms	Business Terms als Grundlage für API-Nutzung
	https://openai.com/policies/service-terms	Service Terms
Modal Labs Inc.	https://modal.com/docs/guide/security	Auflistung von Security Maßnahmen
	https://drive.google.com/file/d/1wwHBsHh-zjwnjcJQ5PR88rYsT4Hxm1Vx/view?usp=sharing	SOC2 Type 1 Report (06/2023)