Anbieter: Summitgo GmbH & Co. KG, Relenbergstraße 65, 70174 Stuttgart · Amtsgericht Stuttgart, HRA 743417 · Persönlich haftende Gesellschafterin: Dr. Mauch Beteiligung GmbH, Sitz Stuttgart, Amtsgericht Stuttgart, HRB 805274, Geschäftsführer Dr. Christian Mauch · USt-IdNr. DE462668169 · info@summitgo.de · https://summitip.de

Stand: 5. November 2026

SUMMITIP · VERTRAGSUNTERLAGEN

Anlage: Technische und organisatorische Maßnahmen

Anlage zum Vertrag zur Auftragsverarbeitung, nach Artikel 32 DSGVO.

Geltungsbereich
Nach Artikel 32 DSGVO treffen Verantwortliche und Auftragsverarbeiter geeignete Maßnahmen, die dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessen sind. Diese Anlage beschreibt, wie SummitGO das für SummiTip umsetzt.
Sie gilt für den SummiTip-Server (Hetzner Online GmbH, Rechenzentrum in Deutschland), die Maschine, die Ton in Text umwandelt (Hetzner Online GmbH, Rechenzentrum in Deutschland), den Sicherungsspeicher bei Hetzner und das Nachlesen des Textes und das Schreiben neuer Fassungen mit Amazon Bedrock in Rechenzentren der Europäischen Union.
Der Vermerk in Klammern nennt, wer eine Maßnahme trägt: SummitGO selbst, die Hetzner Online GmbH (Rechenzentrum und Server), die Amazon Web Services EMEA SARL (Amazon Bedrock) oder die IONOS SE (Mailversand). Die Maßnahmen von Hetzner, Amazon Web Services und IONOS ergeben sich aus deren Verträgen zur Auftragsverarbeitung, Zertifikaten und Testaten.

1 · VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

Zutrittskontrolle
Unbefugte gelangen nicht an die Anlagen, auf denen Daten verarbeitet werden.

TECHNISCHE MASSNAHMEN

- Elektronisches Zutrittskontrollsystem mit Protokollierung (Hetzner)
- Flächendeckende Videoüberwachung, auch der Eingänge (Hetzner)
- Hochsicherheitszaun mit Übersteig- und Untergrabschutz um den Rechenzentrumspark (Hetzner)

ORGANISATORISCHE MASSNAHMEN

- Dokumentierte Vergabe von Zutrittsmedien (Hetzner)
- Richtlinie zum Besuchermanagement (Hetzner)
- Keine eigenen Serverräume: Alle Rechner für SummiTip stehen in Rechenzentren der Hetzner Online GmbH in Deutschland (SummitGO)

1 · VERTRAULICHKEIT

Zugangskontrolle
Unbefugte können die Rechner nicht benutzen.

TECHNISCHE MASSNAHMEN

- Die Server werden über ein Kundenkonto bei Hetzner verwaltet, das ein Kennwort mit Mindestanforderungen verlangt (Hetzner)
- Firewall auf allen Rechnern. Von außen erreichbar sind nur die Internetseite und die Fernwartung (SummitGO)
- Die Festplatten des SummiTip-Servers und der Maschine, die Ton in Text umwandelt, sind vollständig verschlüsselt (SummitGO)
- Der Arbeitsrechner der Geschäftsführung, von dem aus die Server gewartet werden, ist vollständig verschlüsselt (SummitGO)
- Kunden melden sich mit Mailadresse und Einmalcode an. Der Code hat sechs Ziffern, gilt fünfzehn Minuten und erlaubt höchstens fünf Versuche. Gespeichert wird nur ein Prüfwert (SummitGO)
- Im Browser hält ein Cookie die Anmeldung. Es wird nur verschlüsselt übertragen, ist für Skripte nicht lesbar und verfällt nach dreißig Tagen (SummitGO)
- Fernwartung nur über SSH mit Schlüssel. Die Anmeldung mit Kennwort ist abgeschaltet (SummitGO)

ORGANISATORISCHE MASSNAHMEN

- Berechtigungen nach Rollen: Inhaber, Person des Kontos, Betreiber (SummitGO)
- Jede Person meldet sich mit eigener Mailadresse an (SummitGO)
- Löschfristen stehen in § 9 des Vertrags zur Auftragsverarbeitung und in der Datenschutzerklärung und sind im Server umgesetzt (SummitGO)

1 · VERTRAULICHKEIT

Zugriffskontrolle
Wer berechtigt ist, erreicht nur die Daten, für die er berechtigt ist.

TECHNISCHE MASSNAHMEN

- Festgelegtes Löschverfahren für Datenträger nach Vertragsende. Misslingt die Löschung, wird der Datenträger physisch zerstört (Hetzner)
- Änderungen an Wortschatz und Textbausteinen hält der Server mit Person und Zeit fest. Anlage, Kündigung und Löschung eines Kontos stehen im Ereignisbuch des Servers. Ton und Text eines Diktats werden nicht gespeichert (SummitGO)

ORGANISATORISCHE MASSNAHMEN

- Berechtigungskonzept: Die Rollen sind im Server festgelegt (SummitGO)
- Möglichst wenige Verwalter: Der Zugang zu den Servern läuft allein über die Geschäftsführung, am SummiTip-Server ist ein einziger Schlüssel zugelassen (SummitGO)
- Benutzerrechte verwalten nur Betreiber, deren Mailadresse im Verwaltungsportal hinterlegt ist (SummitGO)

1 · VERTRAULICHKEIT

Trennungskontrolle
Daten, die zu verschiedenen Zwecken erhoben wurden, bleiben getrennt.

TECHNISCHE MASSNAHMEN

- Entwickelt und geprüft wird auf dem Arbeitsrechner mit eigener Datenbank. Auf den Server kommt nur ein festgehaltener Stand (SummitGO)
- SummiTip hat eine eigene Datenbank, auf einem Server getrennt vom Betriebsserver der SummitGO Medical Suite (SummitGO)
- Die Daten jedes Kundenkontos sind voneinander getrennt (SummitGO)
- Die Cloud-Server sind logisch voneinander getrennt (Hetzner)
- Der Dienst, der Ton in Text umwandelt, ist von außen nicht erreichbar. Ton erreicht ihn nur über eine verschlüsselte Leitung vom SummiTip-Server (SummitGO)

ORGANISATORISCHE MASSNAHMEN

- Zugriffe richten sich nach dem Berechtigungskonzept (SummitGO)
- Die Datenbank gehört allein dem Dienstkonto im abgeschotteten Programmbehälter. Dieses Konto hat keine Verwalterrechte (SummitGO)

2 · PSEUDONYMISIERUNG (ART. 32 ABS. 1 LIT. A, ART. 25 ABS. 1 DSGVO)

Pseudonymisierung
Daten lassen sich ohne gesondert aufbewahrte Zusatzangaben keiner Person zuordnen.

TECHNISCHE MASSNAHMEN

- Vor dem Nachlesen und vor jeder neuen Fassung ersetzt der SummiTip-Server erkannte Namen und Angaben zu Personen durch Platzhalter, auch in der Beschreibung des Kunden. Die Zuordnung bleibt nur für die Dauer des Aufrufs auf dem Server und geht nicht an Amazon Web Services (SummitGO)

3 · INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)

Weitergabekontrolle
Bei der Übertragung kann niemand die Daten unbefugt lesen, kopieren, verändern oder entfernen, und es ist festgelegt, wohin Daten gehen.

TECHNISCHE MASSNAHMEN

- Je Person und Tag hält der Server die Zahl der Diktate, der Nachlesungen und der neuen Fassungen und ihre Dauer fest, ohne Inhalt, für neunzig Tage (SummitGO)
- Datenträger werden zwischen Standorten nur in verschlossenen Transportboxen bewegt (Hetzner)
- Programm und Internetseite nur über HTTPS mit HSTS, Sicherungen über SFTP, Anfragen an Amazon Web Services über HTTPS (SummitGO)
- Jede Anfrage an Amazon Web Services ist mit dem Verfahren AWS Signature Version 4 signiert (SummitGO)
- Mailversand über IONOS mit Transportverschlüsselung (STARTTLS). Mails enthalten keine Diktate (SummitGO, IONOS)
- Zwischen dem SummiTip-Server und der Maschine, die Ton in Text umwandelt, läuft eine verschlüsselte Leitung (SSH-Tunnel) (SummitGO)

ORGANISATORISCHE MASSNAHMEN

- Die Empfänger stehen in der Liste der Unterauftragnehmer, die Löschfristen in der Datenschutzerklärung (SummitGO)
- Die regelmäßigen Übermittlungen zeigt die Liste der Unterauftragnehmer mit Aufgabe und Ort (SummitGO)
- An Amazon Web Services geht nur Text mit Platzhaltern, nie Ton (SummitGO)

3 · INTEGRITÄT

Eingabekontrolle
Es lässt sich nachträglich feststellen, ob und von wem Daten eingegeben, verändert oder entfernt wurden.

TECHNISCHE MASSNAHMEN

- Wortschatz und Textbausteine tragen Zeit und ändernde Person. Ereignisse eines Kontos stehen im Ereignisbuch, nur mit Mengen (SummitGO)
- Ein Morgenbericht wertet das Ereignisbuch täglich aus (SummitGO)

ORGANISATORISCHE MASSNAHMEN

- Daten eingeben, ändern oder löschen lassen sich nur im Programm SummiTip, auf der Kontoseite und im Verwaltungsportal. Beschrieben ist das in § 2 des Vertrags und in dieser Anlage (SummitGO)
- Persönliche Anmeldung statt Gruppenkonten: Jede Person meldet sich mit eigener Mailadresse an (SummitGO)
- Rechte zur Eingabe, Änderung und Löschung vergibt das Berechtigungskonzept (SummitGO)
- Klare Zuständigkeit für Löschungen: Der Kunde löscht Wortschatz und Konto selbst. Betreiber löschen ein Konto nur nach Eingabe seiner Mailadresse. Die Fristen setzt der tägliche Lauf des Servers um (SummitGO)

4 · VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

Verfügbarkeitskontrolle
Daten sind gegen zufällige Zerstörung und Verlust geschützt.

TECHNISCHE MASSNAHMEN

- Flächendeckende Brandfrüherkennung mit automatischer Alarmierung und Anbindung an eine Leitstelle (Hetzner)
- Ein Mess-, Steuer- und Regelsystem überwacht die Betriebsgrößen der Serverräume (Hetzner)
- Redundante Kühlung und Klimaanlagen (Hetzner)
- Redundante unterbrechungsfreie Stromversorgung und Netzersatzanlagen, redundante Stromeinspeisung (Hetzner)
- Der Sicherungsspeicher speichert redundant (Hetzner)
- Die Serverräume sind videoüberwacht (Hetzner)
- Dynamisches Brandschutzkonzept mit regelmäßig geschulten Brandschutzhelfern (Hetzner)
- Hochverfügbare Netzinfrastruktur, redundant ausgelegt (Hetzner)
- Der Dienst prüft sich selbst und startet nach einer Störung neu (SummitGO)

ORGANISATORISCHE MASSNAHMEN

- Die Kontodaten werden jede Nacht gesichert. Die Sicherungen bleiben sieben Tage am Server und dreißig Tage im Sicherungsspeicher. Dazu gibt es ein Notfallblatt (SummitGO)
- Ein Wächterprogramm prüft jeden Morgen, ob die Sicherung im Sicherungsspeicher liegt (SummitGO)
- Der Sicherungsspeicher steht in einem anderen Rechenzentrum als der SummiTip-Server (SummitGO, Hetzner)
- Notfallplan: Das Notfallblatt nennt Zugänge, Entsperrung und Sicherungsorte (SummitGO)
- Jeden Morgen meldet der Wächter per Mail, ob Server und Umwandlung laufen und ob die Sicherung angekommen ist (SummitGO)
- Technischer Bereitschaftsdienst rund um die Uhr im Rechenzentrum (Hetzner)

5 · REGELMÄSSIGE ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D, ART. 25 ABS. 1 DSGVO)

Datenschutz-Management
Datenschutz und Sicherheit sind organisiert und werden überprüft.

TECHNISCHE MASSNAHMEN

- Hetzner ist nach ISO/IEC 27001:2022 zertifiziert und hat ein Testat nach BSI C5:2020 (Typ 2) (Hetzner)
- Amazon Web Services hat ein Testat nach BSI C5 (Typ 2), Amazon Bedrock steht in dessen Geltungsbereich. SummitGO selbst ist nicht zertifiziert (Amazon Web Services)

ORGANISATORISCHE MASSNAHMEN

- Externer Datenschutzbeauftragter: Herr Till Reichert, e:los GmbH, Heideweg 25, 92318 Neumarkt, datenschutz@elos-net.de, bestellt mit Wirkung zum 1. Oktober 2026 (SummitGO)
- Die Informationspflichten nach Art. 13 und 14 DSGVO erfüllt die Datenschutzerklärung auf summitip.de (SummitGO)

5 · REGELMÄSSIGE ÜBERPRÜFUNG

Umgang mit Sicherheitsvorfällen
Angriffe werden erkannt und abgewehrt.

TECHNISCHE MASSNAHMEN

- Firewall auf allen Rechnern. Sicherheitsaktualisierungen spielt das Betriebssystem selbst ein (SummitGO)
- Nach wiederholten Fehlanmeldungen sperrt ein Schutzprogramm den Absender. Der Server bremst wiederholte Versuche bei Anmeldung und Codes (SummitGO)
- Dauerhaft aktive Erkennung von Überlastungsangriffen (DDoS) (Hetzner)

6 · DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 ABS. 2 DSGVO)

Datenschutz durch Voreinstellung
Es werden nur die Daten verarbeitet, die für den Zweck nötig sind.

TECHNISCHE MASSNAHMEN

- Ton und Text eines Diktats und neue Fassungen werden auf dem Server nicht gespeichert. Ereignisbuch und Zähler enthalten nur Mengen (SummitGO)
- Der Kunde löscht Wortschatz, Bausteine und Konto selbst, im Programm oder auf der Kontoseite (SummitGO)
- Die Aufzeichnung von Ein- und Ausgaben bei Amazon Bedrock ist ausgeschaltet (SummitGO)
- Mit Texten der Kunden werden keine Sprachmodelle trainiert (SummitGO)

7 · AUFTRAGSKONTROLLE

Unterauftragnehmer
Daten, die im Auftrag verarbeitet werden, verarbeiten auch die Unterauftragnehmer nur nach Weisung.

ORGANISATORISCHE MASSNAHMEN

- Verträge, Testate und Zertifikate von Hetzner, Amazon Web Services und IONOS wurden geprüft und sind abgelegt (SummitGO)
- Die Unterauftragnehmer sind nach Datenschutz und Datensicherheit ausgewählt (SummitGO)
- Verträge zur Auftragsverarbeitung: mit Hetzner in der Fassung 1.2, mit Amazon Web Services das Data Processing Addendum mit Standardvertragsklauseln, mit IONOS vom 19. September 2026 (SummitGO, Hetzner, Amazon Web Services, IONOS)
- Die Weisungen an die Unterauftragnehmer stehen in diesen Verträgen (SummitGO)
- Hetzner verpflichtet alle Beschäftigten auf Vertraulichkeit (Hetzner)
- Das Personal von Amazon Web Services ist zur Vertraulichkeit verpflichtet (Amazon Web Services)
- Hetzner und IONOS haben Datenschutzbeauftragte bestellt (Hetzner, IONOS)
- Kontrollrechte: bei Hetzner im Vertrag zur Auftragsverarbeitung, bei Amazon Web Services über Berichte unabhängiger Prüfer (Hetzner, Amazon Web Services)
- Weitere Unterauftragnehmer: bei Hetzner geregelt in Anlage 3 des Vertrags, bei Amazon Web Services mit Ankündigung dreißig Tage vorher (Hetzner, Amazon Web Services)
- Nach Vertragsende werden die Daten gelöscht (Hetzner, Amazon Web Services)