Sendalo startet am 1. Januar 2027. Bis dahin ist keine Anmeldung möglich.

Vertrag zur Auftragsverarbeitung

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen dem Kunden („Verantwortlicher“) und Lautwerk Digital UG (haftungsbeschränkt), vertreten durch den Geschäftsführer Daniel Schenk, Rathausgasse 17, 12529 Schönefeld („Auftragsverarbeiter“). Er wird mit Abschluss des Sendalo-Vertrags (Hauptvertrag) elektronisch vereinbart (Art. 28 Abs. 9 DSGVO) und gilt für dessen Dauer. Stand: 26.10.2026.

1. Gegenstand und Dauer

Der Auftragsverarbeiter stellt dem Verantwortlichen die Software Sendalo bereit und verarbeitet dabei personenbezogene Daten in dessen Auftrag. Die Dauer entspricht der Laufzeit des Hauptvertrags einschließlich der Löschfristen nach Nr. 10. Für Verarbeitungen, bei denen der Auftragsverarbeiter selbst Verantwortlicher ist (z. B. Kundenkonto, Abrechnung), gilt dieser Vertrag nicht.

2. Art und Zweck der Verarbeitung

Speichern, Anzeigen, Veröffentlichen und Auswerten von Social-Media-Inhalten; Abruf und Beantwortung von Kommentaren, Bewertungen und Nachrichten; Website-Chat, WhatsApp, Instagram- und Facebook-Direktnachrichten und E-Mails aus verbundenen Postfächern einschließlich automatischer Antworten durch den KI-Assistenten; Annahme von Anrufen und Mitschrift (Zusatzmodul KI-Telefon); Kommentar-Automationen mit Direktnachrichten; Bereitstellung eines Kundenportals mit Dateien, Freigaben, Nachrichten, elektronischen Unterschriften und Glücksrad; Terminbuchung einschließlich Videotermine; Link-in-Bio-Seiten und Zählen von Linkklicks; Steuerung von Werbeanzeigen; KI-gestützte Erstellung von Texten, Antwortvorschlägen, Alt-Texten, Zusammenfassungen und Berichten; geplante Videomeetings mit Einladungen (auch an externe Personen), Kalenderdateien und Erinnerungen; Newsletter an Kundenportal-Zugänge; E-Mail-Anmeldungen mit Double-Opt-in und Mailings über Link-in-Bio-Seiten; Kontaktverwaltung (CRM) mit Einwilligungen und WhatsApp-Rundsendungen; Engagement-Assistent (Kommentarentwürfe zu eingefügten Beiträgen anderer Accounts); Team-Botschafter (Teilen ausgewählter Beiträge durch Beschäftigte des Verantwortlichen mit Zählung der Teilen-Klicks und Linkklicks je Person); Konkurrenz-Vergleich anhand öffentlicher Kennzahlen; Push-Hinweise; Weiterleitung von Inhalten an vom Verantwortlichen eingerichtete Ziele; Versand von Benachrichtigungen und Buchungsbestätigungen.

3. Arten von Daten und betroffene Personen

- **Daten:** Namen, Kontaktdaten (E-Mail-Adressen, Telefonnummern, WhatsApp-Kennungen), Profilnamen und -bilder, Inhalte von Beiträgen, Kommentaren, Bewertungen, Chats, E-Mails und Anruf-Mitschriften, Kennzahlen zu Beiträgen und Anzeigen, Buchungsdaten, im Kundenportal ausgetauschte Dateien, Nachrichten und Dokumente, Nachweisdaten elektronischer

Unterschriften (Name, Unterschriftsbild, Zeitpunkt, IP-Adresse, Prüfsumme des Dokuments), zufällige Besucher-Kennungen des Website-Chats, Referrer und Zeitpunkt von Linkklicks, Namen, E-Mail-Adressen, Sprache und Einladungsstand von Meeting-Teilnehmenden, Einwilligungsnachweise (Zeitpunkt, Quelle, Wortlaut) für Newsletter, Link-in-Bio-Anmeldungen, WhatsApp- und E-Mail-Werbung, Schlagwörter und Notizen zu Kontakten, Texte und Links von Beiträgen anderer Accounts, die das Team in den Engagement-Assistenten einfügt, Namen, E-Mail-Adressen sowie Teilen- und Klickzahlen von Team-Botschaftern, Namen, Profilbilder und öffentliche Kennzahlen von Wettbewerber-Profilen, Push-Anmeldungen (Adresse beim Push-Dienst, Schlüssel), Nutzungs- und Protokolldaten.

- **Betroffene:** Beschäftigte und Kunden des Verantwortlichen, Follower und Personen, die mit dessen Profilen interagieren, Personen, die dem Verantwortlichen schreiben, ihn anrufen oder den Chat nutzen, Personen, die Termine buchen, Links anklicken oder das Kundenportal nutzen, zu Meetings eingeladene Personen (auch externe), Empfänger von Newslettern, Mailings und Rundsendungen, Kontakte des Verantwortlichen, Verfasser von Beiträgen, die das Team im Engagement-Assistenten bearbeitet, Beschäftigte des Verantwortlichen als Team-Botschafter, Inhaber von Wettbewerber-Profilen.

Besondere Kategorien von Daten (Art. 9 DSGVO) sollen nicht verarbeitet werden. Der Verantwortliche wirkt darauf hin, dass solche Daten nicht in Sendalo eingegeben werden.

4. Weisungen

Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet. Weisungen ergeben sich aus diesem Vertrag und der Nutzung und Einstellung der Funktionen; Einzelweisungen erfolgen in Textform. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit.

5. Vertraulichkeit

Alle Personen mit Zugriff auf die Daten sind zur Vertraulichkeit verpflichtet. Support-Zugriffe auf Daten des Verantwortlichen erfolgen nur nach dessen zeitlich begrenzter Freigabe in der Anwendung und werden protokolliert.

6. Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt. Technische Protokolle, die für die Sicherheit des Dienstes und die Abwehr von Missbrauch nötig sind (z. B. Server-Logdateien), verarbeitet er im Rahmen dieses Auftrags und speichert sie höchstens 7 Tage.

7. Unterauftragsverarbeiter

Der Verantwortliche genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Über neue oder geänderte Unterauftragsverarbeiter informiert der Auftragsverarbeiter mindestens 14 Tage im Voraus in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen; ist eine Einigung nicht möglich, kann er den Hauptvertrag zum Zeitpunkt des Wechsels kündigen. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf gleichwertige Pflichten und haftet für deren Einhaltung nach Art. 28 Abs. 4 DSGVO. Übermittlungen in Drittländer erfolgen nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

8. Unterstützung

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anfragen betroffener Personen (u. a. durch Export- und Löschfunktionen), bei Datenschutz-Folgenabschätzungen und bei der Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO, unter Berücksichtigung der Art der Verarbeitung und der ihm vorliegenden Informationen. Wendet sich eine betroffene Person direkt an ihn, leitet er die Anfrage unverzüglich weiter. Kann der Verantwortliche einzelne Daten (z. B. einen einzelnen Chatverlauf) nicht selbst in der Anwendung löschen, löscht der Auftragsverarbeiter sie auf Weisung.

9. Datenschutzverletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 48 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie vorliegen, und ergänzt sie, sobald weitere Informationen vorliegen.

10. Löschung und Rückgabe

Der Verantwortliche kann seine Daten jederzeit exportieren. Löscht er sein Konto, löscht der Auftragsverarbeiter die Daten sofort; endet der Hauptvertrag auf andere Weise, kann der Verantwortliche seine Daten noch 30 Tage lang exportieren, danach werden sie gelöscht. Dies gilt jeweils, soweit keine Pflicht zur Speicherung nach Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Datensicherungen (auch die verschlüsselte Kopie außer Haus) werden spätestens nach 30 Tagen gelöscht bzw. überschrieben. Auf Anfrage bestätigt der Auftragsverarbeiter die Löschung in Textform.

11. Nachweise und Kontrollen

Der Auftragsverarbeiter stellt alle zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlichen Informationen bereit, vorrangig durch aktuelle Dokumentation der Maßnahmen und Nachweise der Unterauftragsverarbeiter. Er ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer, der kein Wettbewerber des Auftragsverarbeiters ist. Vor-Ort-Prüfungen sind nach

angemessener Ankündigung zu den üblichen Geschäftszeiten möglich; jede Partei trägt ihre eigenen Kosten.

12. Rechte und Pflichten des Verantwortlichen

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Rechte der betroffenen Personen verantwortlich, insbesondere für die Information der Betroffenen (Art. 13, 14 DSGVO) und für erforderliche Einwilligungen. Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

13. Haftung und Schlussbestimmungen

Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln des Hauptvertrags. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in Fragen des Datenschutzes vor.

Anlage 1 – Technische und organisatorische Maßnahmen

- **Zutrittskontrolle:** Betrieb ausschließlich in Rechenzentren der STRATO AG in Deutschland mit Zutrittsschutz rund um die Uhr (nach ISO/IEC 27001 zertifizierte Rechenzentren). Keine Server in Büroräumen. Einzige Ausnahme ist die Ende-zu-Ende-verschlüsselte Kopie der Datensicherung außer Haus (siehe „Sicherung außer Haus“).
- **Zugangskontrolle:** Server-Zugang nur per SSH-Schlüssel, Passwort-Anmeldung deaktiviert, Firewall mit nur den nötigen Ports, automatische Sperre nach Fehlversuchen, Zwei-Faktor-Anmeldung für Verwaltungskonten; in der Anwendung Login-Sperre, widerrufbare Sitzungen und optional verpflichtende Zwei-Faktor-Anmeldung für das Team.
- **Zugriffskontrolle:** Rollen (Admin, Redaktion, Nur lesen, Kundenportal), strikte Trennung der Mandanten in der Anwendung; Kundenportal-Zugänge sehen nur Daten ihres eigenen Kunden; Portal-Dateien liegen außerhalb des öffentlichen Webverzeichnisses und werden nur nach Rechteprüfung ausgeliefert; Support-Zugriff nur mit Freigabe des Kunden und mit Protokoll.
- **Weitergabekontrolle:** Übertragung ausschließlich per TLS (HTTPS); Verbindungen zu E-Mail-Servern nur mit TLS. Zugriffstokens der Plattformen, WhatsApp-Zugangsdaten, Passwörter verbundener E-Mail-Postfächer, eigene API-Schlüssel und Zwei-Faktor-Geheimnisse werden mit AES-256-GCM verschlüsselt gespeichert; Zugangsdaten im Passwort-Safe des Kundenportals zusätzlich mit eigenem Schlüssel, Anzeige nur nach erneuter Bestätigung und mit Protokoll (ohne Wert), nie im Support-Zugriff; Passwörter der Nutzer nur als scrypt-Hash.
- **Eingabekontrolle:** Protokollierung von Anmeldungen, Rechteänderungen, Veröffentlichungen und Support-Zugriffen; Aufbewahrung der Protokolle 2 Jahre.
- **Verfügbarkeit:** Tägliche verschlüsselte Datensicherung (AES-256), Aufbewahrung höchstens 30 Tage, Wiederherstellung wird regelmäßig getestet; Überwachung der Dienste; zeitnahes Einspielen von Sicherheitsupdates.

- **Sicherung außer Haus:** Zusätzlich wird jede Nacht eine Kopie der Datensicherung auf einem eigenen Speichergerät (NAS) des Auftragsverarbeiters in Deutschland abgelegt. Die Kopie wird noch auf dem Server mit age Ende-zu-Ende-verschlüsselt; der private Schlüssel liegt weder auf dem Server noch auf dem Speichergerät, sondern offline beim Inhaber. Das Speichergerät holt die Kopie über eine verschlüsselte SSH-Verbindung ab (eigener Zugang nur mit Schlüssel, nur lesend und nur auf die verschlüsselten Dateien, Prüfung des Server-Schlüssels); am Standort des Speichergeräts ist kein Zugang aus dem Internet geöffnet. Das Speichergerät steht in nicht öffentlich zugänglichen Räumen, Zugang zu Gerät und Daten hat nur der Inhaber, die Datenträger sind verschlüsselt. Aufbewahrung höchstens 30 Tage.
- **Trennungskontrolle:** Daten verschiedener Kunden sind logisch getrennt; Entwicklungs- und Testumgebungen nutzen keine Echtdaten.
- **Datensparsamkeit:** Server-Logdateien und technische Protokolle werden nach 7 Tagen gelöscht, Zugangsschlüssel in Adressen (z. B. Freigabe-, Kalender- und Meeting-Links) nicht mitgeschrieben; Portal-Dateien nach der vom Verantwortlichen eingestellten Frist; geplante Meetings mit Einladungen 30 Tage nach dem Termin bzw. der Absage; Versandlisten von Newslettern 30 Tage nach dem Versand; Linkklicks werden ohne IP-Adresse gezählt; Verbindungsaufbau für Videotermine nur über den eigenen STUN/TURN-Server.
- **Überprüfung:** Die Maßnahmen werden mindestens jährlich und nach wesentlichen Änderungen überprüft und dokumentiert.

Anlage 2 – Unterauftragsverarbeiter

DIENSTLEISTER	LEISTUNG	ORT DER VERARBEITUNG
STRATO AG, Berlin	Hosting von Anwendung, Datenbank, Datensicherungen und Videoserver, E-Mail-Versand	Deutschland
Anthropic Ireland, Limited, Dublin (mit Anthropic PBC, San Francisco)	KI-Funktionen (Texte, Antworten, Alt-Texte, Zusammenfassungen, Berichte, Chat-Assistent, KI-Telefon, Kommentarentwürfe im Engagement-Assistenten); keine Nutzung der Daten zum Training	Irland/USA – EU-Standardvertragsklauseln (Module 2 und 3)
sipgate GmbH, Düsseldorf	Rufnummern, Anrufannahme, Sprache ↔ Text (sipgate AI Flow) für das KI-Telefon (Zusatzmodul)	Deutschland/EU

DIENSTLEISTER	LEISTUNG	ORT DER VERARBEITUNG
└ verda (Unterauftragsverarbeiter von sipgate)	Rechenzentrum für sipgate AI Flow	Helsinki, Finnland (EU)
└ Microsoft Ireland Operations Ltd., Dublin (Unterauftragsverarbeiter von sipgate)	Spracherkennung und Sprachausgabe (Microsoft Azure Cognitive Services)	Irland (EU)

sipgate lässt den Anbieter für Spracherkennung und Sprachausgabe je Gespräch wählen. Sendalo stellt dafür ausschließlich Microsoft Azure (Microsoft Ireland Operations Ltd.) ein; die Sprachverarbeitung ist damit nicht mit einer Übermittlung in die USA verbunden. Der Auftragsverarbeitungsvertrag von sipgate nennt außerdem Eleven Labs Inc., New York (USA), für Spracherkennung und Sprachausgabe – diesen Anbieter wählt Sendalo nicht aus. Die jeweils aktuelle Liste der Unterauftragsverarbeiter von sipgate stellt der Anbieter auf Anfrage zur Verfügung.

Die Schnittstellen sozialer Netzwerke und der WhatsApp Business Platform (Meta mit Facebook, Instagram, Threads und WhatsApp, TikTok, Google, LinkedIn, Pinterest, Bluesky, Snapchat, X) sowie der E-Mail-Anbieter verbundener Postfächer, der Telefonanbieter des Verantwortlichen und die Ziele, an die der Verantwortliche selbst Inhalte übermitteln lässt (Slack, Microsoft Teams, ausgehende Webhooks, Zugriffe mit seinen Schlüsseln über die Schnittstelle API v1 und über MCP), sind keine Unterauftragsverarbeiter: Der Verantwortliche nutzt diese Dienste auf Grundlage eigener Verträge bzw. veranlasst die Übermittlung selbst, Sendalo übermittelt die Inhalte in seinem Auftrag dorthin. Hinterlegt der Verantwortliche einen eigenen Claude-API-Schlüssel, nutzt er Anthropic auf Grundlage seines eigenen Vertrags. Die Kopie der Datensicherung außer Haus speichert der Auftragsverarbeiter auf eigener Hardware in Deutschland (Anlage 1, Sicherung außer Haus); dafür setzt er keinen Unterauftragsverarbeiter ein. Push-Hinweise werden über den Push-Dienst zugestellt, den der Browser bzw. das Gerät der jeweiligen Nutzer vorgibt; die Inhalte sind dabei Ende-zu-Ende-verschlüsselt.