

Datenschutzmappe

alkaio – WhatsApp AI Sales Agent

MindLike UG (haftungsbeschränkt) Kurhessenstraße 3b, 63075 Offenbach am Main, Deutschland Amtsgericht Offenbach am Main, HRB 50940 · Geschäftsführer: Abdul Wahed Hemati, Tolga Uslu Telefon: +49 69 257 297 430 · E-Mail: hello@alkaio.com · Web: alkaio.com

Stand: 6. August 2026

Diese Datenschutzmappe fasst die zentralen datenschutzrechtlichen Informationen zur Nutzung von alkaio für unsere Geschäftskund:innen zusammen. Sie unterstützt Kund:innen dabei, ihren Dokumentations- und Rechenschaftspflichten nach der DSGVO nachzukommen, wenn sie alkaio als Auftragsverarbeiter einsetzen.

Die Mappe enthält:

1. Überblick und Rollenverteilung
2. Datenfluss (Wie verarbeitet alkaio Daten?)
3. Datenschutzrechtliche Einordnung der WhatsApp Cloud API
4. Vertrag über die Auftragsverarbeitung (AVV, Art. 28 DSGVO)
5. Anhang 1 – Einzelheiten der Auftragsverarbeitung
6. Anhang 2 – Liste der Unterauftragsverarbeiter
7. Anhang 3 – Technische und organisatorische Maßnahmen (TOMs)

1. Überblick und Rollenverteilung

alkaio ist eine KI-gestützte Software-as-a-Service-Lösung der MindLike UG (haftungsbeschränkt), mit der Unternehmen ihre Vertriebs- und Kommunikationsprozesse über WhatsApp und weitere Kanäle automatisieren. Der AI Sales Agent führt Konversationen mit Endkund:innen, qualifiziert Leads und unterstützt die Terminierung und Weiterbearbeitung.

Datenschutzrechtliche Rollen

- Die **Kundin/der Kunde** (das die Plattform nutzende Unternehmen) ist **Verantwortliche:r** im Sinne des Art. 4 Nr. 7 DSGVO für die über alkaio verarbeiteten personenbezogenen Daten ihrer/seiner Endkund:innen. Sie/er entscheidet über Zwecke und Mittel der Verarbeitung, konfiguriert die Flows und ist für die Rechtsgrundlage und die Information der betroffenen Personen verantwortlich.
- Die **MindLike UG** ist **Auftragsverarbeiterin** im Sinne des Art. 28 DSGVO. Sie verarbeitet die Daten ausschließlich weisungsgebunden zur Bereitstellung der Leistung.
- Die eingesetzten Dienstleister (siehe Anhang 2) sind **Unterauftragsverarbeiter**. Meta/WhatsApp ist im Rahmen der Cloud API (Unter-)Auftragsverarbeiterin; für die von WhatsApp erhobenen Metadaten ist WhatsApp datenschutzrechtlich selbst verantwortlich.

2. Datenfluss – Wie verarbeitet alkaio Daten?

Der typische Datenfluss einer Konversation über alkaio stellt sich wie folgt dar:

1. **Endkund:in – WhatsApp:** Die Endkundin/der Endkunde startet über QR-Code, Link oder Telefonnummer eine Unterhaltung. Die Nachricht wird von der WhatsApp-App Ende-zu-Ende verschlüsselt an die WhatsApp-Plattform übertragen.
2. **WhatsApp – Meta Cloud API:** Die Nachricht wird an die WhatsApp Business Platform (Cloud API) der Meta Platforms Ireland Limited übermittelt und dort entschlüsselt. Die Cloud API speichert Inhalte nur vorübergehend (in der Regel höchstens 30 Tage); die lokale Datenspeicherung erfolgt in Rechenzentren innerhalb der EU bzw. in Deutschland. Beim Transport können Nachrichten technisch über Server außerhalb der EU geleitet werden; Inhalte im Transit werden nach kurzer Zeit automatisch gelöscht.
3. **Meta Cloud API – alkaio (STRATO, Deutschland):** Die Nachricht wird an die alkaio-Plattform übergeben, die auf einem Server der STRATO AG (Rechenzentren in Deutschland, IONOS-Gruppe) betrieben wird; der Website ist Cloudflare als Content-Delivery-Network/Reverse-Proxy vorgeschaltet. Dort werden die Nachricht, der Konversationskontext und die zugehörigen Lead-Daten gespeichert und verarbeitet.
4. **alkaio – KI-Anbieter:** Zur Erzeugung einer passenden Antwort werden die relevanten Nachrichten- und Kontextinhalte an ein KI-Sprachmodell (OpenAI, Anthropic oder Google) übergeben. Die Anbieter verarbeiten die Inhalte ausschließlich weisungsgebunden zur Erbringung der Leistung und nicht zum Training eigener Modelle. Bei einer Übermittlung in die USA bestehen geeignete Garantien nach Art. 44 ff. DSGVO.
5. **Antwort zurück an die Endkund:in:** Die erzeugte Antwort wird über die Cloud API und WhatsApp an die Endkundin/den Endkunden zurückgesendet.
6. **Verwaltung & Abrechnung:** Kontodaten der Kundin/des Kunden werden zur Verwaltung des Accounts (STRATO, Deutschland) sowie zur Zahlungsabwicklung (Stripe) verarbeitet.

Schematisch:

Endkund:in $\rightleftharpoons$ WhatsApp (E2E) $\rightleftharpoons$ Meta Cloud API (EU/DE) $\rightleftharpoons$ Cloudflare (CDN/Proxy) $\rightleftharpoons$ alkaio $\cdot$ STRATO Deutschland (EU) $\rightleftharpoons$ KI-Anbieter (OpenAI / Anthropic / Google)

3. Datenschutzrechtliche Einordnung der WhatsApp Cloud API

Hinweis: Dieser Abschnitt stellt die datenschutzrechtliche Einordnung der MindLike UG als Anbieterin dar. Er dient der Information und ersetzt keine individuelle Rechtsberatung. Kund:innen wird empfohlen, die Nutzung im eigenen Verantwortungsbereich rechtlich prüfen zu lassen.

Zusammenfassung. Nach unserer Einschätzung ermöglicht die Nutzung der WhatsApp Business Plattform über die Cloud API Unternehmen eine datenschutzkonforme geschäftliche Nutzung des WhatsApp-Messengers.

Keine Synchronisierung von Kontaktdaten. Bei der Nutzung von WhatsApp Business über die Cloud API entfällt der Einsatz einer WhatsApp-Applikation auf einem Endgerät des Unternehmens. Dadurch kommt es nicht zu der Synchronisierung von Kontaktdaten (Adressbuchabgleich), die in der Vergangenheit der zentrale Kritikpunkt deutscher Datenschutzbehörden am Einsatz von WhatsApp war.

Rollenverteilung. Die Cloud API und alkaio als Business Solution Provider fungieren als Zwischenstelle zwischen WhatsApp und dem Kunden. Der Kunde ist datenschutzrechtlich Verantwortlicher. MindLike ist Auftragsverarbeiterin des Unternehmens und Meta wiederum (Unter-)Auftragsverarbeiterin im Sinne des Art. 28 DSGVO. Der Einsatz von Auftragsverarbeitern bei der Verarbeitung ist nach Art. 28 DSGVO zulässig, sofern entsprechende vertragliche, organisatorische und technische Maßnahmen bestehen.

Verschlüsselung und Rolle der Cloud API. Die WhatsApp-Kommunikation über die Cloud API ist durch Verschlüsselungsmaßnahmen abgesichert, die dem Stand der Technik entsprechen. Nachrichten werden zwischen Nutzer und Cloud API verschlüsselt übertragen; die Cloud API verwendet branchenübliche Verschlüsselungsverfahren, um Daten während der Übertragung und im Ruhezustand zu sichern. Ruhende Nachrichten werden spätestens nach 30 Tagen automatisch gelöscht.

Lokale Speicherung. Für Kund:innen, die WhatsApp über die Cloud API nutzen, kann die lokale Datenspeicherung in der EU bzw. in Deutschland aktiviert werden. Dass Nachrichten unter Umständen über einen Server außerhalb der EU transportiert werden, ist mit Blick auf die Zertifizierung von Meta unter dem EU-US Data Privacy Framework gerechtfertigt (Art. 45 Abs. 1 DSGVO); Inhalte im Transit werden kurzfristig automatisch gelöscht.

Metadaten. Für die Verarbeitung der von WhatsApp erhobenen Metadaten (z. B. Zeitpunkt, Häufigkeit und Dauer der Nutzung, Geräte- und Verbindungsinformationen) ist nach verbreiteter Auffassung WhatsApp selbst verantwortlich. Die bloße Nutzung von WhatsApp durch Unternehmen begründet insoweit regelmäßig keine gemeinsame Verantwortlichkeit, da das Unternehmen auf die Verarbeitung der Metadaten nicht aktiv einwirkt und die verfolgten Zwecke sich unterscheiden.

Drittlandübermittlung. Soweit Metadaten an die WhatsApp LLC oder Meta Platforms, Inc. in den USA weitergeleitet werden, ist diese Übermittlung nach Art. 45 Abs. 1 DSGVO gerechtfertigt, da die Empfänger unter dem EU-US Data Privacy Framework zertifiziert sind.

Empfehlung an Kund:innen. Kund:innen sollten in ihrer eigenen Datenschutzerklärung und in den Kommunikationsprozessen die betroffenen Personen transparent über die Nutzung von

WhatsApp und die Verarbeitung informieren (Art. 13/14 DSGVO) und eine geeignete Rechtsgrundlage sicherstellen.

Vertrag über die Auftragsverarbeitung (Art. 28 Abs. 3 DSGVO)

MindLike UG (haftungsbeschränkt) – alkaio Stand: 6. August 2026

Dieser Vertrag über die Auftragsverarbeitung („Vertrag“ oder „AVV“) gilt zwischen dem Kunden (nachfolgend bezeichnet als „Auftraggeberin“) und der

MindLike UG (haftungsbeschränkt), Kurhessenstraße 3b, 63075 Offenbach am Main, Amtsgericht Offenbach am Main HRB 50940, Steuernummer 4423923950, vertreten durch die Geschäftsführer Abdul Wahed Hemati und Tolga Uslu (jeweils einzelvertretungsberechtigt) (nachfolgend bezeichnet als „Auftragnehmerin“).

Die Parteien haben einen Nutzungsvertrag über die Software „alkaio“ (WhatsApp AI Sales Agent) abgeschlossen. In Ergänzung zum Nutzungsvertrag vereinbaren die Parteien hiermit Folgendes. Dieser Vertrag wird mit Registrierung und Abschluss des Nutzungsvertrags durch die Auftraggeberin – einschließlich der Bestätigung der Allgemeinen Geschäftsbedingungen und dieses AVV im Registrierungsprozess – wirksam.

1. Gegenstand des Vertrages und der Verarbeitung, Umfang der Weisungsbefugnisse

1.1 Gegenstand dieses Vertrages ist die Zusammenarbeit der Parteien im Rahmen des Nutzungsvertrages. Die Durchführung des Nutzungsvertrages beinhaltet die in **Anhang 1** benannten datenverarbeitenden Tätigkeiten der Auftragnehmerin für die Auftraggeberin.

1.2 Die Auftragnehmerin verarbeitet die ihr im Rahmen des Nutzungsvertrages zugänglichen personenbezogenen Daten im Auftrag der Auftraggeberin (Art. 28 DSGVO). Die Auftragnehmerin wird die Daten ausschließlich und streng nach den auftragsbezogenen Weisungen der Auftraggeberin verarbeiten, berichtigen und nutzen; die Ziele und Modalitäten der Auftragsverarbeitung kann allein die Auftraggeberin bestimmen.

1.3 Die Verantwortung für das Erstellen und Umsetzen des Löschkonzepts, die Durchführung des Rechts auf Vergessenwerden, auf Berichtigung, Datenportabilität und Auskunft sind nicht Gegenstand dieses Vertrages. Diese wird allein durch die Auftraggeberin sichergestellt.

1.4 Die vereinbarte Verarbeitungstätigkeit durch die Auftragnehmerin findet grundsätzlich innerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt. Sofern Verarbeitungstätigkeiten durch Unterauftragnehmer in Drittländern erbracht werden, ist dies in **Anhang 2** entsprechend aufgeführt und es gilt für die betreffende Drittlandübermittlung entweder ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO oder es sind Standarddatenschutzklauseln mit sonstigen geeigneten Garantien nach Art. 46 DSGVO abgeschlossen.

1.5 Außerhalb der Betriebsstätte der Auftragnehmerin findet folgende Datenverarbeitung statt: Die Auftragnehmerin erlaubt ihren Mitarbeitern die Arbeit aus dem Home-Office. Hierfür gelten bei der Auftragnehmerin Regelungen zum Datenschutz, auf deren Einhaltung sich die Mitarbeiter verpflichtet haben.

2. Art und Zweck der Verarbeitung

2.1 Für die Durchführung des Nutzungsvertrages mit der Auftraggeberin ist der Zugriff auf personenbezogene Daten notwendig.

2.2 Die Zwecke der Auftragsverarbeitung sind in **Anhang 1** benannt. Die Auftragsverarbeitung erfolgt nur für die Zwecke der Durchführung des Nutzungsvertrages mit der Auftraggeberin; eine Verwendung für andere Zwecke erfolgt nicht. Den Mitarbeitern der Auftragnehmerin ist es untersagt, geschützte personenbezogene Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten oder zu nutzen.

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1 Die Arten der personenbezogenen Daten, die von der Datenverarbeitung durch die Auftragnehmerin betroffen sind, sind in **Anhang 1** aufgelistet.

3.2 Die Personengruppen, die zum Kreis der durch die Verarbeitung betroffenen Personen gehören, sind in **Anhang 1** aufgelistet.

4. Rechte und Pflichten der Auftraggeberin

4.1 Die Prüfung der Zulässigkeit der Datenverarbeitung und die Wahrung der Rechte der Betroffenen obliegen stets der Auftraggeberin. Die Auftraggeberin übernimmt die ihr nach den Datenschutzbestimmungen obliegenden Meldepflichten in eigener Verantwortung (Art. 33, 34 DSGVO).

4.2 Die Auftraggeberin bestätigt mündlich erteilte Weisungen stets in Textform oder in einer zwischen den Parteien vereinbarten sonstigen elektronischen Form. Änderungen des Verarbeitungsgegenstandes oder Verfahrensänderungen stimmt die Auftraggeberin vorab gemeinsam mit der Auftragnehmerin ab; die Parteien treffen hierzu eine entsprechende Festlegung in Textform.

4.3 Für die Auftraggeberin sind die in **Anhang 1** genannten Personen gegenüber der Auftragnehmerin berechtigt, auftragsbezogene Weisungen zu erteilen.

4.4 Die Auftraggeberin wird die Auftragnehmerin über den Wechsel einer nach Ziffer 4.3 benannten Person in geeigneter Form informieren.

4.5 Die Auftraggeberin ist berechtigt, bei der Auftragnehmerin jederzeit die Einhaltung der Datenschutzbestimmungen und der getroffenen vertraglichen Vereinbarungen und erteilten Weisungen zu überprüfen. Die Einzelheiten der Kontrollrechte regelt Ziffer 11.

4.6 Die Auftraggeberin hat das Recht, jederzeit die Herausgabe der im Rahmen dieses Vertrages verarbeiteten und/oder neu entstandenen Daten, Daten-Ergebnisse oder Datenbestände zu verlangen. Alle Rechte und das Eigentum an diesen Daten, Datenergebnissen oder Datenbeständen stehen allein der Auftraggeberin als Inhaberin und allein berechtigter Eigentümerin zu. Die Auftragnehmerin hat diesbezüglich kein Zurückbehaltungsrecht (§§ 273, 320 BGB). Etwaige urheberrechtliche Nutzungs- oder Lizenzrechte (z. B. an der Software) bleiben davon unberührt.

5. Weitere Rechte und Pflichten der Auftragnehmerin

5.1 Die in **Anhang 1** genannten Personen sind für die Auftragnehmerin befugt, Weisungen der Auftraggeberin entgegenzunehmen.

5.2 Die Auftragnehmerin wird die in Ziffer 3 bzw. **Anhang 1** dieses Vertrages genannten personenbezogenen Daten nur nach dokumentierter Weisung der Auftraggeberin verarbeiten, berichtigen, löschen oder sperren. Sie wird die Auftraggeberin nach Möglichkeit bei der Erfüllung der Pflichten zu den Rechten betroffener Personen (Art. 12 bis 23 DSGVO) unterstützen. Soweit eine betroffene Person sich unmittelbar an die Auftragnehmerin zwecks Berichtigung oder Löschung der eigenen personenbezogenen Daten wenden sollte, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

5.3 Die Auftragnehmerin führt ein eigenes Verzeichnis über die Verarbeitungstätigkeit (Art. 30 Abs. 2 DSGVO). Sie wird bei der Erstellung von Verzeichnissen über die Verarbeitungstätigkeit und Datenschutz-Folgenabschätzungen der Auftraggeberin mitwirken und der Auftraggeberin die dafür benötigten Informationen – soweit möglich und bei der Auftragnehmerin vorhanden – bereitstellen. Darüber hinaus wird die Auftragnehmerin die Auftraggeberin im Rahmen ihrer Möglichkeiten bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO unterstützen.

5.4 Alle Unterlagen und/oder Datenträger und/oder Datenbestände der Auftraggeberin wird die Auftragnehmerin so verwahren, dass sie von denjenigen weiterer Kunden der Auftragnehmerin getrennt und vor der Kenntnis bzw. dem Zugriff Unbefugter geschützt sind.

5.5 Die Auftragnehmerin hat, soweit gesetzlich verpflichtet, eine geeignete Person als Beauftragte für den Datenschutz bestellt (Art. 37 DSGVO). Die Kontaktdaten sind in **Anhang 1** genannt. Sollte ein Datenschutzbeauftragter bestellt oder gewechselt werden, wird die Auftragnehmerin die Auftraggeberin unverzüglich darüber unterrichten.

5.6 Die Auftragnehmerin wird die Auftraggeberin von auftragsbezogenen Störungen im Betriebsablauf, Verletzungen von Datenschutzbestimmungen (auch durch Weisungen der Auftraggeberin), Kontrollen und Maßnahmen der Aufsichtsbehörden und anderen Unregelmäßigkeiten unverzüglich unterrichten. Die Auftragnehmerin unterstützt die Auftraggeberin bei der Erfüllung der Meldepflichten, die der Auftraggeberin im Fall von Datenschutzverletzungen (Art. 33, 34 DSGVO) obliegen.

5.7 Macht eine betroffene Person oder ein Dritter einen Anspruch im Zusammenhang mit der vorliegenden Auftragsverarbeitung gegen die Auftragnehmerin geltend, wird die Auftragnehmerin die Auftraggeberin um die zur Verfügung stehenden Informationen unterstützen.

5.8 Die Auftragnehmerin ist berechtigt, die Durchführung von Weisungen, die nach Ansicht der Auftragnehmerin Datenschutzbestimmungen verletzen, solange auszusetzen, bis die Auftraggeberin diese bestätigt oder geändert hat.

6. Technische und organisatorische Maßnahmen

6.1 Die Auftragnehmerin hat im Zeitpunkt des Abschlusses dieses Vertrages bereits nachweislich alle für den vorliegenden Auftrag nach Art. 32 DSGVO erforderlichen und

angemessenen technischen und organisatorischen Maßnahmen (TOM) zur Datensicherheit getroffen, die die Auftraggeberin akzeptiert hat. Diese sind in **Anhang 3** zu diesem Vertrag im Einzelnen beschrieben und entsprechen dem in Art. 32 Abs. 1 DSGVO geregelten Maßnahmenkatalog. **Anhang 3** zu diesem Vertrag wird hiermit Vertragsbestandteil.

6.2 Bei der Auswahl der konkreten TOM wird die Auftragnehmerin folgende Kriterien berücksichtigen: den Stand der Technik; die Implementierungskosten; die Art, den Umfang, die Umstände und die Zwecke der vorliegenden Verarbeitung; die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen natürlichen Personen.

6.3 Die Auftragnehmerin verpflichtet sich, stets ein angemessenes Schutzniveau der betroffenen TOM zu gewährleisten. Bei der Auswahl der konkreten TOM nach Ziffer 6.2 gewährleistet die Auftragnehmerin ein dem Risiko angemessenes Schutzniveau u. a. durch: Pseudonymisierung und Verschlüsselung der personenbezogenen Daten; dauerhafte Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung; Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen bei einem physischen oder technischen Zwischenfall; ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.

6.4 Der Auftragnehmerin ist es gestattet, die einmal getroffenen konkreten TOM im Zuge des technischen Fortschritts und der Weiterentwicklung durch modernere TOM zu ersetzen, die den in den Ziffern 6.2 und 6.3 dieses Vertrages vereinbarten Kriterien entsprechen und stets ein angemessenes Schutzniveau gewährleisten. Wesentliche Änderungen sind zu dokumentieren.

7. Geheimhaltung

7.1 Die Vertragsparteien verpflichten sich gegenseitig, während der Laufzeit dieses Vertrages und für die Dauer von einem Jahr nach Beendigung dieses Vertrages alle ihnen im Rahmen der Durchführung dieser Vereinbarung bekannt gewordenen Informationen und Kenntnisse über die jeweils andere Partei, die Beschäftigten- und Kundendaten sowie Entwürfe, Konzepte, Methoden und der sonstige Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln.

7.2 Die der jeweils anderen Partei zugänglich gemachten Unterlagen bleiben Eigentum der betreffenden Partei und sind streng vertraulich zu behandeln. Sie dürfen ohne schriftliche Einwilligung der betreffenden Vertragspartei weder vervielfältigt, veröffentlicht, noch auf sonstige Weise Dritten zugänglich gemacht werden und dürfen nicht für einen anderen als für den vereinbarten Zweck verwendet werden.

7.3 Ausgenommen von der Geheimhaltungspflicht sind nicht geschützte Ideen, Konzeptionen, Erfahrungen sowie Informationen, die einer Vertragspartei bereits vorab bekannt waren oder öffentlich bekannt oder offenkundig sind oder ohne Verschulden der Vertragspartei bekannt werden.

8. Verpflichtung zur Vertraulichkeit (Datengeheimnis)

8.1 Die Vertragsparteien werden personenbezogene Daten nur nach Maßgabe der jeweils geltenden datenschutzrechtlichen Bestimmungen erheben, verarbeiten und nutzen. Die Vertragsparteien verpflichten sich gegenseitig zur Wahrung des Datengeheimnisses.

8.2 Jede Partei wird die eigenen, zur Datenverarbeitung eingesetzten Mitarbeiter vor Durchführung der Arbeiten auf das Datengeheimnis verpflichten (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO) und über die einschlägigen Datenschutzbestimmungen in Kenntnis setzen.

8.3 Die Weitergabe personenbezogener Daten und/oder von sonstigen Informationen aus dem Bereich der Auftragnehmerin an Dritte ist der Auftragnehmerin verboten, es sei denn, sie erfolgt auf Grundlage von Ziffer 9 (Unterauftragsverhältnisse) oder aufgrund einer dokumentierten Weisung der Auftraggeberin.

9. Unterauftragsverhältnisse

9.1 Die Auftraggeberin erteilt der Auftragnehmerin die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragnehmer) im Sinne des Art. 28 Abs. 2 und 4 DSGVO einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer sind in **Anhang 2** benannt und werden von der Auftraggeberin genehmigt.

9.2 Beabsichtigt die Auftragnehmerin, einen weiteren Unterauftragnehmer hinzuzuziehen oder einen bestehenden zu ersetzen, informiert sie die Auftraggeberin hierüber in geeigneter Form (z. B. per E-Mail oder durch Aktualisierung der jeweils online abrufbaren Liste) mit einer angemessenen Vorlauffrist. Die Auftraggeberin kann der Änderung aus wichtigem, datenschutzrechtlich begründetem Grund innerhalb von 14 Tagen widersprechen. Im Falle eines berechtigten Widerspruchs sind die Parteien berechtigt, den Vertrag hinsichtlich der betroffenen Leistung außerordentlich zu kündigen.

9.3 Die Auftragnehmerin wird die datenschutzrechtlichen Verpflichtungen dieses Vertrages den Unterauftragnehmern in gleichem Umfang vertraglich auferlegen (Art. 28 Abs. 4 DSGVO) und diese sorgfältig, insbesondere im Hinblick auf die Eignung ihrer technischen und organisatorischen Maßnahmen, auswählen.

9.4 Werden Verarbeitungstätigkeiten durch Unterauftragnehmer in Drittländern erbracht, stellt die Auftragnehmerin durch geeignete Garantien nach Art. 44 ff. DSGVO ein angemessenes Datenschutzniveau sicher (Angemessenheitsbeschluss oder Standarddatenschutzklauseln nebst ergänzenden Maßnahmen). Die eingesetzten Unterauftragnehmer sowie die jeweilige Grundlage der Drittlandübermittlung sind in **Anhang 2** angegeben.

9.5 Nicht als Unterauftragsverhältnis im Sinne dieser Ziffer gelten Nebenleistungen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt (z. B. Telekommunikations-, Reinigungs- oder Wartungsleistungen), sofern kein Zugriff auf personenbezogene Daten der Auftraggeberin besteht.

10. Rechte betroffener Personen

10.1 Die Auftragnehmerin unterstützt die Auftraggeberin nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, ihrer Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO nachzukommen.

10.2 Wendet sich eine betroffene Person unmittelbar an die Auftragnehmerin, leitet die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiter und wird selbst nicht ohne Weisung tätig.

11. Kontroll- und Prüfrechte der Auftraggeberin

11.1 Die Auftragnehmerin stellt der Auftraggeberin alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die von der Auftraggeberin oder einem von dieser beauftragten Prüfer durchgeführt werden.

11.2 Die Auftragnehmerin kann dem Kontrollrecht der Auftraggeberin durch Übermittlung eines aktuellen Datenschutzberichts, genehmigter Verhaltensregeln (Art. 40 DSGVO) oder eines genehmigten Zertifikats oder Datenschutzsiegels bzw. Datenschutzprüfzeichens im Sinne von Art. 42 DSGVO genügen.

11.3 Überprüfungen vor Ort werden rechtzeitig angekündigt, finden während der üblichen Geschäftszeiten statt und dürfen den Betriebsablauf der Auftragnehmerin nicht unverhältnismäßig beeinträchtigen. Die Kosten für über den üblichen Umfang hinausgehende Unterstützungsleistungen kann die Auftragnehmerin nach vorheriger Ankündigung angemessen in Rechnung stellen.

12. Mitteilung bei Verstößen und Meldepflichten

12.1 Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich, nachdem ihr eine Verletzung des Schutzes personenbezogener Daten der Auftraggeberin bekannt geworden ist. Die Mitteilung enthält, soweit möglich, die in Art. 33 Abs. 3 DSGVO genannten Angaben.

12.2 Die Auftragnehmerin trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und unterrichtet die Auftraggeberin hierüber.

13. Löschung und Rückgabe von personenbezogenen Daten

13.1 Nach Abschluss der Verarbeitungstätigkeiten oder auf Weisung der Auftraggeberin – jedenfalls mit Beendigung des Nutzungsvertrages – hat die Auftragnehmerin sämtliche personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

13.2 Die Löschung wird der Auftraggeberin auf Anforderung in geeigneter Form nachgewiesen. Bestehende gesetzliche Aufbewahrungspflichten bleiben unberührt; entsprechende Daten werden für die weitere Verarbeitung gesperrt.

14. Laufzeit und Beendigung

14.1 Dieser Vertrag beginnt mit Abschluss des Nutzungsvertrages und ist auf die Dauer des Nutzungsvertrages befristet. Er endet automatisch mit Beendigung des Nutzungsvertrages, ohne dass es einer gesonderten Kündigung bedarf.

14.2 Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn die Auftragnehmerin ihren Pflichten aus diesem Vertrag schwerwiegend zuwiderhandelt, eine Weisung der Auftraggeberin nicht ausführt oder den Zutritt der Auftraggeberin oder der Aufsichtsbehörde zu Kontrollzwecken vertragswidrig verweigert.

15. Haftung

15.1 Für die Haftung gelten die Regelungen des Art. 82 DSGVO. Im Verhältnis der Parteien untereinander gelten ergänzend die Haftungsregelungen des Nutzungsvertrages bzw. der AGB, soweit diese nicht zwingenden datenschutzrechtlichen Vorgaben widersprechen.

16. Schlussbestimmungen

16.1 Sollten sich einzelne Bestimmungen dieses Vertrages als unwirksam oder undurchführbar erweisen oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der datenschutzrechtlichen Zielsetzung am nächsten kommen.

16.2 Bei Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen der Parteien, insbesondere dem Nutzungsvertrag, gehen die Regelungen dieses Vertrages vor. Im Zweifel gehen die Regelungen der DSGVO vor.

16.3 Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Es gilt das Recht der Bundesrepublik Deutschland.

Anhang 1 – Einzelheiten der Auftragsverarbeitung

Gegenstand des Auftrags Bereitstellung und Betrieb der Software „alkaio“ (WhatsApp AI Sales Agent) als Software-as-a-Service zur Automatisierung von Vertriebs- und Kommunikationsprozessen der Auftraggeberin, einschließlich der Verarbeitung der über die Plattform ein- und ausgehenden Kommunikation.

Art und Zweck der Verarbeitung Erhebung, Speicherung, Organisation, Verwendung, Auslesen, Abfrage, Übermittlung (an eingesetzte Unterauftragnehmer nach Anhang 2), Löschung und Vernichtung personenbezogener Daten zum Zweck des Betriebs des AI Sales Agent, der Führung und Anreicherung von Leads, der automatisierten und teilautomatisierten Kommunikation über WhatsApp und weitere Kanäle sowie der Bereitstellung der zugehörigen Auswertungs- und Verwaltungsfunktionen.

Dauer der Verarbeitung Für die Laufzeit des Nutzungsvertrages sowie bis zur vertragsgemäßen Löschung oder Rückgabe der Daten (Ziffer 13).

Art der personenbezogenen Daten

- Kontakt- und Stammdaten (z. B. Name, Telefonnummer, E-Mail-Adresse, Anschrift)
- Kommunikations- und Nachrichteninhalte (Chatverläufe über WhatsApp und weitere Kanäle)
- Lead- und Vertriebsdaten (z. B. Interessen, Status, Qualifizierungsangaben, im Flow erhobene Angaben)
- Metadaten der Kommunikation (z. B. Zeitstempel, Kanal, technische Verbindungsdaten)
- ggf. weitere von der Auftraggeberin über die Flow-Konfiguration erhobene Angaben (z. B. Tarif-, Bedarfs- und Vertragsangaben)

Hinweis: Die Auftraggeberin ist dafür verantwortlich, dass über die Plattform keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) erhoben werden, soweit hierfür keine Rechtsgrundlage besteht und keine ergänzenden Schutzmaßnahmen vereinbart wurden.

Kategorien betroffener Personen

- Endkund:innen, Interessent:innen und Leads der Auftraggeberin
- Kontakte und Ansprechpartner:innen der Auftraggeberin
- ggf. Beschäftigte der Auftraggeberin, soweit sie die Plattform nutzen

Weisungsberechtigte Personen der Auftraggeberin [Name(n) und Kontaktdaten der weisungsberechtigten Person(en) der Auftraggeberin – regelmäßig die im Kundenkonto hinterlegte administrierende Person.]

Weisungsempfänger der Auftragnehmerin Die Geschäftsführung der MindLike UG bzw. die von ihr benannte Ansprechperson, erreichbar unter hello@alkaio.com.

Datenschutzbeauftragte:r der Auftragnehmerin Ein Datenschutzbeauftragter ist nicht bestellt, da die gesetzlichen Voraussetzungen für eine Benennungspflicht (§ 38 BDSG) nicht vorliegen. Kontakt in Datenschutzangelegenheiten: hello@alkaio.com.

Anhang 2 – Liste der Unterauftragsverarbeiter (Unterauftragnehmer)

Die Auftragnehmerin setzt zum Zeitpunkt des Vertragsschlusses die nachfolgenden Unterauftragnehmer ein. Mit allen Unterauftragnehmern bestehen Verträge zur Auftragsverarbeitung nach Art. 28 DSGVO.

A. Verarbeitung im Rahmen der Bereitstellung und des Betriebs von alkaio

Firma, Anschrift	Art und Zweck der Verarbeitung	Art der Daten	Kategorien betroffener Personen	Ort der Verarbeitung / Drittlandgarantie
STRATO AG, Otto-Ostrowski- Straße 7, 10249 Berlin, Deutschland	Bereitstellung des Servers für Plattform, Datenbank und Speicher	Alle vorgenannten Datenarten	Endkunden, Kontakte und Mitarbeiter der Auftraggeberin	Deutschland. Rechenzentren in Deutschland (IONOS-Gruppe), ISO 27001 zertifiziert. Keine Drittlandübermittlung.
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA (EU- Vertretung: Cloudflare Germany GmbH, München)	Content Delivery Network, DNS, TLS und Angriffsschutz; leitet sämtliche Anfragen inkl. WhatsApp-Webhook durch	IP-Adressen, Verbindungsdaten und durchgeleitete Nachrichteninhalte	Websitebesucher sowie Endkunden und Mitarbeiter der Auftraggeberin	EU-Rechenzentren; Drittlandbezug USA über Standarddatenschutzklauseln (SCC) bzw. EU-US Data Privacy Framework.
Meta Platforms Ireland Limited / WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland	Bereitstellung der WhatsApp Business Plattform (Cloud API), Übermittlung der Nachrichten	Telefonnummer, Nachrichteninhalte, Metadaten der Kommunikation	Endkunden und Kontakte der Auftraggeberin	EU (lokale Speicherung EU/DE); Transport ggf. über USA. Angemessenheitsbeschluss (EU-US DPF) / SCC.
OpenAI Ireland Ltd., 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1,	KI-gestützte Erzeugung automatisierter Antworten	Nachrichten- und Kontextinhalte der Kommunikation	Endkunden und Kontakte der Auftraggeberin	EU/USA. Angemessenheitsbeschluss (EU-US DPF) / SCC. Keine Nutzung zum

Firma, Anschrift	Art und Zweck der Verarbeitung	Art der Daten	Kategorien betroffener Personen	Ort der Verarbeitung / Drittlandgarantie
Irland (bzw. OpenAI, L.L.C., USA)				Modelltraining.
Anthropic PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, USA	KI-gestützte Erzeugung automatisierter Antworten	Nachrichten- und Kontextinhalte der Kommunikation	Endkunden und Kontakte der Auftraggeberin	USA. SCC / EU-US DPF. Keine Nutzung zum Modelltraining.
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (Google Cloud / Vertex AI)	KI-gestützte Erzeugung automatisierter Antworten	Nachrichten- und Kontextinhalte der Kommunikation	Endkunden und Kontakte der Auftraggeberin	EU/USA. Angemessenheitsbeschluss (EU-US DPF) / SCC. Keine Nutzung zum Modelltraining.
Google Ireland Limited (Google Workspace/Gmail), Gordon House, Barrow Street, Dublin 4, Irland	Versand von System- und Transaktions-E-Mails	Name, E-Mail-Adresse	Nutzer:innen / Kontakte der Auftraggeberin	EU/USA. Angemessenheitsbeschluss (EU-US DPF) / SCC.

B. Verarbeitung im Rahmen der Verwaltung und Betreuung des Kundenaccounts der Auftraggeberin

Firma, Anschrift	Art und Zweck der Verarbeitung	Art der Daten	Kategorien betroffener Personen	Ort der Verarbeitung / Drittlandgarantie
Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland	Zahlungsabwicklung und Abrechnung der Abonnements	Name, Rechnungs- und Zahlungsdaten von Mitarbeiter:innen der Auftraggeberin	Mitarbeiter:innen der Auftraggeberin	EU/USA. Angemessenheitsbeschluss (EU-US DPF) / SCC.
STRATO AG, Otto-Ostrowski-Straße 7, 10249	Hosting der Verwaltungs-/Kontodaten	Konto- und Stammdaten der Auftraggeberin	Mitarbeiter:innen der Auftraggeberin	EU (Deutschland). Keine

Firma, Anschrift	Art und Zweck der Verarbeitung	Art der Daten	Kategorien betroffener Personen	Ort der Verarbeitung / Drittlandgaranti e
Berlin, Deutschland	(Server in Deutschland, IONOS-Gruppe)			Drittlandübermi ttlung.

Die jeweils aktuelle Fassung dieser Liste stellt die Auftragnehmerin unter <https://alkaio.com/dpa.html> bereit. Änderungen werden gemäß Ziffer 9.2 mitgeteilt.

Anhang 3 – Technische und organisatorische Maßnahmen der Auftragnehmerin (Art. 32 DSGVO)

Beschreibung der technischen und organisatorischen Maßnahmen der MindLike UG (haftungsbeschränkt).

1. Zusammenfassung der getroffenen Maßnahmen

- Maßnahmen zur Verschlüsselung von Daten bei der Übertragung (TLS) und im Ruhezustand (Verschlüsselung auf Speicher- und Datenbankebene).
- Dauerhafte Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste; die Vertraulichkeit ist durch Zutritts-, Zugangs- und Zugriffskontrolle gewährleistet, die Integrität durch Absicherung der eingesetzten Systeme (u. a. Firewalls, restriktive Berechtigungen), die Verfügbarkeit durch Back-ups und die Belastbarkeit durch die eingesetzte Serverinfrastruktur.
- Fähigkeit zur raschen Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach einem physischen oder technischen Zwischenfall über Backups; das genutzte Rechenzentrum (STRATO, Deutschland, IONOS-Gruppe) verfügt über Notstromversorgung und Ausfallsicherheit.
- Automatisiertes, dauerhaftes Monitoring der Systeme sowie regelmäßige Überprüfung der Wirksamkeit der Maßnahmen.

2. Allgemeine organisatorische Maßnahmen

- Beschäftigte werden vertraglich zur Vertraulichkeit und auf das Datengeheimnis verpflichtet (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO) und über die rechtlichen Konsequenzen bei Zuwiderhandlung belehrt.
- Es besteht eine dokumentierte Systemkonfiguration und ein Berechtigungskonzept.
- Verträge zur Auftragsverarbeitung werden mit allen Dienstleistern abgeschlossen (Art. 28 DSGVO); sorgfältige Auswahl der Unterauftragnehmer.
- Sicherheitsvorfälle werden dokumentiert und ausgewertet.

3. Zutrittskontrolle *(Verhinderung des Zutritts Unbefugter zu Datenverarbeitungsanlagen)*

- Betrieb in einem ISO-27001-zertifizierten Rechenzentrum der STRATO AG (IONOS-Gruppe) in Deutschland mit umfassenden physischen Zutrittskontrollen; kein eigener Serverraum-Betrieb.
- Für Büroräume: verschlossene Räumlichkeiten, Zutritt nur für berechtigte Personen.

4. Zugangskontrolle *(Verhinderung der Nutzung der Systeme durch Unbefugte)*

- Authentifikation mit Benutzername/Passwort; Passwortrichtlinie (Mindestlänge, Komplexität).
- Multi-Faktor-Authentifizierung für administrative Zugänge.
- Einsatz von Firewalls und aktueller Sicherheitssoftware; verschlüsselte Endgeräte.
- Vergabe personenbezogener Benutzerprofile; „Clean Desk“-Prinzip.

5. Zugriffskontrolle *(Beschränkung auf berechtigte Daten)*

- Rollen- und rechtebasiertes Berechtigungskonzept; Zugriff nach dem Need-to-know-Prinzip.
- Anzahl administrativer Zugänge auf das notwendige Minimum begrenzt.
- Protokollierung von Zugriffen; Verfahren zum Entzug von Berechtigungen bei Ausscheiden.

6. Weitergabekontrolle (*Schutz bei Übertragung und Transport*)

- Verschlüsselung sämtlicher Datenübertragungen (TLS/HTTPS).
- Vorgelagertes Content-Delivery-Network / Reverse-Proxy mit WAF- und DDoS-Schutz (Cloudflare).
- Mandantengetrennte Datenhaltung; Übermittlung an Unterauftragnehmer nur auf vertraglicher Grundlage (Art. 28 DSGVO).

7. Eingabekontrolle (*Nachvollziehbarkeit von Eingaben/Änderungen*)

- Die eingesetzten IT-Systeme verfügen über Protokollierungsfunktionen (Logging), die nachvollziehbar machen, durch wen Daten eingegeben, verändert oder entfernt wurden.

8. Auftragskontrolle (*weisungsgemäße Verarbeitung*)

- Verträge zur Auftragsverarbeitung mit allen Dienstleistern (Art. 28 DSGVO).
- Sorgfältige Auswahl und Prüfung der Unterauftragnehmer, insbesondere im Hinblick auf Datensicherheit.

9. Verfügbarkeitskontrolle (*Schutz vor Zerstörung und Verlust*)

- Regelmäßige Backups; Speicherung an einem sicheren Ort.
- Serverinfrastruktur in einem Rechenzentrum mit Notstromversorgung und Ausfallsicherheit (STRATO, Deutschland, IONOS-Gruppe).
- Konzept zur Sicherung und Wiederherstellung von Daten (Backup/Restore/Recovery).

10. Trennungskontrolle (*getrennte Verarbeitung nach Zweck/Mandant*)

- Logische Trennung der Datenbestände nach Mandanten (Kunden).
- Trennung von Produktiv- und Testsystem; Steuerung über Berechtigungskonzept.

11. Überprüfung

- Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO).

Unterschriften

Sofern dieser Vertrag nicht bereits mit der Online-Registrierung und Bestätigung im Rahmen des Nutzungsvertrages wirksam geschlossen wurde, kann er von den Parteien wie folgt gesondert gezeichnet werden:

Für die Auftraggeberin (Kunde)

Ort, Datum: _____

Name / Funktion: _____

Unterschrift: _____

Für die Auftragnehmerin (MindLike UG (haftungsbeschränkt))

Ort, Datum: _____

Name / Funktion: _____

Unterschrift: _____