mailgrado.com

Vertrag über die Auftragsverarbeitung

nach Art. 28 der Datenschutz-Grundverordnung (DSGVO) · Fassung vom 08.10.2026

zwischen

Firma, Rechtsform

Anschrift

Vertreten durch (Name, Funktion)

– nachfolgend **„Auftraggeber“** –

und

StartSmartLife, Inhaber Leon Weber
Barkhof 10a, 48356 Nordwalde
E-Mail: support@mailgrado.com
Betreiber des Dienstes mailgrado.com

– nachfolgend **„Auftragnehmer“** –

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer überträgt für den Auftraggeber über den Dienst mailgrado.com E-Mail-Postfächer von einem bisherigen zu einem neuen Postfach-Anbieter („Umzug“). Grundlage sind die Aufträge, die der Auftraggeber über mailgrado.com erteilt, sowie die Allgemeinen Geschäftsbedingungen des Auftragnehmers („Hauptvertrag“). Dieser Vertrag regelt die datenschutzrechtlichen Pflichten beider Parteien, soweit der Auftragnehmer dabei personenbezogene Daten im Auftrag verarbeitet.

(2) Der Vertrag gilt für alle Umzüge, die der Auftraggeber ab Unterzeichnung beauftragt, und endet, wenn für keinen dieser Umzüge mehr Daten beim Auftragnehmer verarbeitet werden (§ 9). Er kann von beiden Seiten mit einer Frist von einem Monat in Textform gekündigt werden; bereits laufende Umzüge werden nach diesem Vertrag abgewickelt.

§ 2 Art und Zweck der Verarbeitung, Datenarten, Betroffene

(1) Zweck: Übertragung der Inhalte der vom Auftraggeber benannten Postfächer in die vom Auftraggeber benannten Zielpostfächer, einschließlich der dafür nötigen Vorprüfung, Fortschrittsanzeige und Benachrichtigung.

(2) Art der Verarbeitung: Abrufen, Übertragen und Ablegen. Postfach-Inhalte werden ausschließlich flüchtig im Arbeitsspeicher vom Quell- zum Zielpostfach übertragen und nicht dauerhaft gespeichert, nicht protokolliert und nicht ausgewertet. Auf das Quellpostfach wird nur lesend zugegriffen.

(3) Datenarten:

- **Zugangsdaten:** Postfach-Adressen, Passwörter oder Zugriffs-Token, Serverangaben;
- **Inhalte:** E-Mails einschließlich Anhängen und Metadaten (Absender, Empfänger, Betreff, Zeitpunkte), bei Umzügen von Microsoft 365 zu Microsoft 365 zusätzlich Kontakte, Termine und Aufgaben. Die Inhalte können besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie Daten enthalten, die einem Berufsgeheimnis unterliegen;
- **Protokolldaten:** Ordnernamen, Anzahl und Datenmenge der Nachrichten, Fortschritt sowie bei nicht übertragenen E-Mails Ordner, Datum, Größe und Grund – nie Betreff, Absender oder Inhalt.

(4) Betroffene: Inhaber und Nutzer der Postfächer (insbesondere Beschäftigte des Auftraggebers) sowie deren Kommunikationspartner (z. B. Kunden, Mandanten, Patienten, Lieferanten und sonstige Dritte).

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist gesetzlich zu einer anderen Verarbeitung verpflichtet; in diesem Fall teilt er dies dem Auftraggeber vorab mit, sofern das Gesetz dies nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen sind der einzelne Umzugsauftrag, dieser Vertrag und der Hauptvertrag. Weitere Weisungen erteilt der Auftraggeber in Textform an support@mailgrado.com.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin und darf die Ausführung bis zur Klärung aussetzen.

§ 4 Vertraulichkeit und Berufsgeheimnisse

(1) Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind. Derzeit verarbeitet ausschließlich der Inhaber selbst Daten; weitere Personen werden vor Aufnahme ihrer Tätigkeit schriftlich zur Vertraulichkeit verpflichtet.

(2) Unterliegt der Auftraggeber einer beruflichen Schweigepflicht (z. B. als Rechtsanwalt, Steuerberater, Arzt), wirkt der Auftragnehmer an dessen beruflicher Tätigkeit mit. Er verpflichtet sich, fremde Geheimnisse, die ihm dabei bekannt werden, geheim zu halten und sich nur insoweit Kenntnis zu verschaffen, als dies für den Umzug erforderlich ist. Er ist darüber belehrt, dass eine unbefugte Offenbarung nach § 203 Abs. 4 StGB strafbar ist. Personen, die er künftig zur Verarbeitung einsetzt, verpflichtet er vor Aufnahme ihrer Tätigkeit in Textform entsprechend.

(3) Hinweis zu den Unterauftragsverarbeitern (Anlage 2): Mit ihnen bestehen Auftragsverarbeitungsverträge nach Art. 28 DSGVO, die sie unter anderem zur Verarbeitung nur auf Weisung und zur Verpflichtung ihres Personals auf Vertraulichkeit verpflichten. Eine gesonderte Verschwiegenheitsverpflichtung im Sinne von § 203 Abs. 4 StGB, § 43e BRAO oder § 62a StBerG haben sie bislang nicht abgegeben; der Auftragnehmer hat sie beim Hoster angefragt und teilt dem Auftraggeber in Textform mit, sobald sie vorliegt. Der Hoster stellt ausschließlich Rechenzentrum, Hardware und Netzanbindung bereit, verwaltet den Server nicht und greift nach seinem Vertrag nur ausnahmsweise (z. B. bei einem Hardwaretausch) auf gespeicherte Daten zu; ausgesonderte Datenträger werden nach DIN 66399 vernichtet. Postfach-Inhalte werden nicht auf dem Server gespeichert (§ 2 Abs. 2), Zugangsdaten nur verschlüsselt und nur bis zum Abschluss des Umzugs (§ 9 Abs. 2, Anlage 1). Microsoft erhält für den Versand der Status-E-Mails keine Postfach-Inhalte. Unterliegt der Auftraggeber einer beruflichen Schweigepflicht, entscheidet er in eigener Verantwortung, ob er den Dienst unter diesen Voraussetzungen nutzt.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO.

(2) Er darf die Maßnahmen an die technische Entwicklung anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vorab in Textform über die Hinzuziehung oder den Austausch weiterer Unterauftragsverarbeiter. Der Auftraggeber kann innerhalb

dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen; kann keine Einigung erzielt werden, dürfen beide Parteien diesen Vertrag und den Hauptvertrag für künftige Umzüge kündigen.

(3) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen; für Verschwiegenheitsverpflichtungen nach § 203 StGB gilt § 4 Abs. 3.

(4) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind die Postfach-Anbieter des Auftraggebers (z. B. Microsoft, Google, IONOS), zu denen der Auftraggeber in eigener Vertragsbeziehung steht, sowie der Zahlungsdienstleister Stripe, der ausschließlich Zahlungsdaten des Auftraggebers verarbeitet.

§ 7 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Art. 12 bis 22 DSGVO). Wendet sich eine betroffene Person direkt an ihn, leitet er die Anfrage unverzüglich an den Auftraggeber weiter.

(2) Er unterstützt den Auftraggeber bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation), soweit ihm die dafür nötigen Informationen vorliegen.

§ 8 Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, in Textform. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Der Auftragnehmer ergreift unverzüglich Maßnahmen zur Eindämmung und informiert den Auftraggeber über deren Stand.

§ 9 Löschung und Rückgabe

(1) Postfach-Inhalte werden vom Auftragnehmer nicht gespeichert; sie liegen nach dem Umzug weiterhin unverändert im Quellpostfach und im Zielpostfach des Auftraggebers.

(2) Zugangsdaten löscht der Auftragnehmer automatisch: sofort nach erfolgreichem Umzug, bei gebuchtem Delta-Sync spätestens 14 Tage danach, bei fehlgeschlagener Vorprüfung sofort, ohne Zahlung spätestens nach 24 Stunden und bei fehlgeschlagenen Umzügen nach 7 Tagen.

(3) Protokolldaten und übrige Auftragsdaten löscht er automatisch 30 Tage nach Erstellung des Auftrags (unbezahlte Aufträge nach 7 Tagen). Datensicherungen werden spätestens nach 30 Tagen überschrieben. Auf Weisung des Auftraggebers löscht er früher und bestätigt die Löschung in Textform.

(4) Gesetzliche Aufbewahrungspflichten des Auftragnehmers (z. B. für Rechnungen) bleiben unberührt; sie betreffen keine Postfach-Inhalte.

§ 10 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind.

(2) Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer darf die Einhaltung nach rechtzeitiger Anmeldung – in der Regel 14 Tage vorab – während der üblichen Geschäftszeiten überprüfen. Vorrangig erfolgt die Überprüfung durch schriftliche Auskünfte und Unterlagen; Überprüfungen vor Ort beschränken sich auf die Räumlichkeiten des Auftragnehmers, da der Server in einem Rechenzentrum des Hosters betrieben wird.

§ 11 Ort der Verarbeitung

Die Verarbeitung findet in Deutschland statt; der Server steht in einem Rechenzentrum in Deutschland. Eine Verarbeitung in Drittländern außerhalb der EU erfolgt nur, soweit dies in Anlage 2 angegeben ist und die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 12 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen richtet sich die Haftung nach dem Hauptvertrag.

§ 13 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

(2) Änderungen und Ergänzungen bedürfen der Textform. Die Anlagen sind Bestandteil dieses Vertrags.

(3) Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Es gilt das Recht der Bundesrepublik Deutschland.

Unterschriften

Auftraggeber	**Auftragnehmer**
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:
Name, Funktion:	Leon Weber, Inhaber StartSmartLife

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: 06.10.2026

1. Vertraulichkeit

- **Zutrittskontrolle:** Der Server steht in einem Rechenzentrum des Hosters WIIT AG (ehemals myLoc managed IT AG) in Deutschland; der physische Zutritt ist durch den Hoster geregelt. Der Auftragnehmer betreibt keine eigenen Serverräume; Arbeitsgeräte befinden sich in abgeschlossenen Räumen.
- **Zugangskontrolle:** Verwaltungszugang zum Server ausschließlich per SSH-Schlüssel, Anmeldung per Passwort ist deaktiviert. Die Verwaltungsoberfläche der Virtualisierung ist nicht aus dem Internet erreichbar. Firewall: von außen nur SSH sowie HTTPS/HTTP der Website erreichbar.
- **Zugriffskontrolle:** Zugriff auf Auftragsdaten hat nur der Inhaber. Der Verwaltungsbereich der Website ist durch Passwort und einen zweiten Faktor (Einmalcode) geschützt und gegen massenhafte Anmeldeversuche begrenzt. Datenbank und Zwischenspeicher sind nicht aus dem Internet erreichbar.
- **Trennungskontrolle:** Jeder Auftrag wird als eigener Datensatz mit zufälliger, nicht erratbarer Kennung geführt; Zugangsdaten sind je Auftrag getrennt verschlüsselt.
- **Verschlüsselung:** Zugangsdaten werden mit AES-256-GCM verschlüsselt gespeichert; der Schlüssel liegt nicht in der Datenbank.

2. Integrität

- **Weitergabekontrolle:** Alle Verbindungen sind verschlüsselt: Website per HTTPS (TLS), Postfach-Zugriff per IMAP ausschließlich über TLS 1.2 oder höher (STARTTLS verpflichtend), Microsoft 365 und Google über deren verschlüsselte Schnittstellen. Unverschlüsselte Verbindungen zu Postfächern werden nicht aufgebaut.
- **Eingabekontrolle:** Der Ablauf jedes Umzugs wird protokolliert (Zeitpunkt, Ordner, Anzahl, Fehler) – ohne Postfach-Inhalte, Betreffzeilen oder Absender.
- **Datensparsamkeit:** Postfach-Inhalte werden nur flüchtig im Arbeitsspeicher übertragen und nie auf Datenträgern abgelegt; auf das Quellpostfach wird nur lesend zugegriffen. Es gibt keine Zugriffsprotokolle mit IP-Adressen; technische Fehlermeldungen des Webservers enthalten nur gekürzte IP-Adressen.

3. Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbank und der Serverkonfiguration, wöchentliche Sicherung des gesamten Systems; Kopien an einem zweiten, räumlich getrennten Ort in Deutschland in einem verschlüsselten Speicher (AES-256).
- Die Wiederherstellung aus der Sicherung wurde am 30.09.2026 vollständig getestet.
- Abgebrochene Umzüge werden automatisch am letzten übertragenen Stand fortgesetzt; bei Verbindungsabbrüchen verbindet sich der Dienst selbstständig neu.
- Automatische Sicherheitsupdates der Betriebssysteme von Server und Virtualisierungshost; die Sicherungen werden protokolliert und regelmäßig kontrolliert.

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Prüfung der Sicherheitseinstellungen (u. a. HTTPS-Konfiguration, Sicherheits-Header, E-Mail-Authentifizierung per SPF, DKIM und DMARC, DNSSEC).
- Automatische Tests der Software vor jeder Veröffentlichung.
- Löschfristen werden automatisch durchgesetzt (siehe § 9 des Vertrags).

Anlage 2 – Unterauftragsverarbeiter

Stand: 06.10.2026

Unternehmen	Leistung	Verarbeitete Daten	Ort
WIIT AG (ehemals myLoc managed IT AG, Marke ServerDiscount), Düsseldorf	Bereitstellung und Betrieb des Servers (Rechenzentrum, Hardware, Netzanbindung)	alle in § 2 genannten Daten, soweit auf dem Server verarbeitet; Zugriff nur ausnahmsweise (z. B. Hardwaretausch)	Deutschland
WIIT S.p.A., Mailand (Unterauftragnehmer der WIIT AG)	Zentrale Unternehmensleistungen der Muttergesellschaft des Hosters	nur soweit für diese Leistungen im Einzelfall erforderlich	Italien (EU)
Microsoft Ireland Operations Limited, Dublin	Versand der Status-E-Mails zum Auftrag (Microsoft 365)	Postfach-Adressen, Anzahl der E-Mails, Link zur Statusseite	EU (EU Data Boundary)

Postfach-Anbieter des Auftraggebers und der Zahlungsdienstleister Stripe sind keine Unterauftragsverarbeiter (§ 6 Abs. 4).