RECHTLICHES

Auftragsverarbeitungsvereinbarung

Version
v2026-12-01
Gültig ab
1. Dezember 2026
SHA-256
1f8b7c5cce1e7ff34c2d4cb83ae18faa97aa1dcd0f4043dd6675c6ec85312b3c

Unverbindliche Übersetzung. Maßgeblich ist die englische Fassung (English version prevails).

> Unverbindliche Übersetzung. Maßgeblich ist die englische Fassung.

Auftragsverarbeitungsvereinbarung (Schedule 3 zu den Customer Terms of Service)

Version v2026-12-01 · Gültig ab 1. Dezember 2026

Diese Auftragsverarbeitungsvereinbarung („AVV“) ist Bestandteil der Customer Terms of Service der PUSH - CONSULTING LLC (die „Terms“) sowie jedes darunter geschlossenen Order Form und Statement of Work („SOW“) (zusammen der „Vertrag“). Der Kunde nimmt diese AVV zusammen mit den Terms an. Eine gesonderte Unterschrift ist nicht erforderlich. Diese AVV gilt ab dem ersten Hochladen, Eingeben oder sonstigen Verarbeiten personenbezogener Daten über die Services, auch während einer Testphase (Trial).

Parteien sind:

- der in seinem Growmino-One-Konto, Order Form oder SOW bezeichnete Kunde („Kunde“); und
- PUSH - CONSULTING LLC, eine Limited Liability Company nach dem Recht des US-Bundesstaats Wyoming, 30 N Gould St Ste N, Sheridan, WY 82801, USA, Wyoming Secretary of State Filing ID 2026-002106936, vertreten durch ihren Sole Member und Manager David Wolff, office@growmino.de, tätig unter den Marken „Growmino“ und „Growmino One“ („Anbieter“).

Diese AVV enthält alle nach Art. 28 Abs. 3 DSGVO erforderlichen Regelungen. Sie gilt vollständig aus sich heraus, unabhängig davon, ob für einen bestimmten

Verarbeitungsvorgang die Standardvertragsklauseln (Abschnitt 11) anwendbar sind.

---

1. Begriffsbestimmungen

1.1 In dieser AVV nicht definierte großgeschriebene Begriffe haben die Bedeutung aus den Terms. Die Begriffe „Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“, „personenbezogene Daten“, „Verarbeitung“, „Aufsichtsbehörde“ und „Verletzung des Schutzes personenbezogener Daten“ haben die Bedeutung aus der DSGVO; ihre Entsprechungen in anderen Datenschutzgesetzen sind entsprechend auszulegen.

1.2 In dieser AVV bedeuten:

- **„Kunden-personenbezogene Daten“** personenbezogene Daten in den Kundendaten, die der Anbieter im Rahmen des Vertrags im Auftrag des Kunden verarbeitet.
- **„Vom Kunden verbundene Dienste“** Dienste Dritter, die der Kunde oder seine Authorised Users auf Grundlage eines eigenen Vertrags mit dem jeweiligen Dritten mit den Services verbinden, insbesondere die eigenen Google-Workspace- oder Google-Konten, Microsoft-365- oder Outlook-Konten, eigene Twilio-Konten, eigene Werbekonten (etwa Google Ads oder Meta) und eigene Integrationswerkzeuge (etwa Zapier) des Kunden.
- **„Datenschutzgesetze“** alle auf die Verarbeitung der Kunden-personenbezogenen Daten im Rahmen des Vertrags anwendbaren Datenschutzgesetze, einschließlich der DSGVO, der sie umsetzenden oder ergänzenden Gesetze der EU-Mitgliedstaaten, der UK GDPR und des UK Data Protection Act 2018, des Schweizer Bundesgesetzes über den Datenschutz vom 25. September 2020 („DSG“ bzw. „FADP“) sowie der US-Bundesstaaten-Datenschutzgesetze.
- **„DPF“** das EU-U.S. Data Privacy Framework, die UK-Erweiterung des EU-U.S. Data Privacy Framework und das Swiss-U.S. Data Privacy Framework, jeweils soweit einschlägig, zusammen mit den hierzu ergangenen Angemessenheitsbeschlüssen oder Anerkennungen.
- **„DSGVO“** die Verordnung (EU) 2016/679.
- **„Personenbezogene Daten“** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, sowie alle Informationen, die nach Datenschutzgesetzen als „personal data“, „personal information“ oder mit einem gleichwertigen Begriff definiert sind.
- **„Verletzung des Schutzes personenbezogener Daten“** eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu Kunden-personenbezogenen Daten führt, die vom Anbieter oder seinen Unterauftragsverarbeitern übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
- **„Beschränkte Übermittlung“** eine Übermittlung von Kunden-personenbezogenen Daten an ein Drittland oder eine internationale Organisation, die Kapitel V DSGVO, den

entsprechenden Regeln der UK GDPR oder Art. 16 und 17 DSG unterliegt.

- **„SCC“** die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer im Anhang zum Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021.
- **„Unterauftragsverarbeiter“** jeder vom Anbieter beauftragte Auftragsverarbeiter, der im Zusammenhang mit den Services Kunden-personenbezogene Daten im Auftrag des Anbieters verarbeitet.
- **„UK Addendum“** das International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, herausgegeben vom UK Information Commissioner nach Section 119A UK Data Protection Act 2018, in Kraft seit 21. März 2022, in der jeweils geltenden Fassung.
- **„US-Bundesstaaten-Datenschutzgesetze“** der California Consumer Privacy Act in der durch den California Privacy Rights Act geänderten Fassung („CCPA“) und vergleichbare Datenschutzgesetze von US-Bundesstaaten, soweit anwendbar.

---

2. Anwendungsbereich und Rollen der Parteien

2.1 **Kunde als Verantwortlicher.** Soweit der Kunde über Zwecke und Mittel der Verarbeitung der Kunden-personenbezogenen Daten entscheidet, ist der Kunde Verantwortlicher und der Anbieter sein Auftragsverarbeiter.

2.2 **Kunde als Auftragsverarbeiter.** Soweit der Kunde Kunden-personenbezogene Daten im Auftrag eines dritten Verantwortlichen verarbeitet (etwa eine Agentur, die die Services für ihre eigenen Kunden nutzt), ist der Kunde Auftragsverarbeiter und der Anbieter Unterauftragsverarbeiter des Kunden. Der Kunde sichert zu, dass sein Verantwortlicher die Weisungen des Kunden nach dieser AVV genehmigt hat, einschließlich der Beauftragung des Anbieters und der in Anlage 3 aufgeführten Unterauftragsverarbeiter. Der Kunde ist alleiniger Ansprechpartner des Anbieters. Der Anbieter ist nicht verpflichtet, direkt mit dem Verantwortlichen des Kunden zu kommunizieren, es sei denn, Datenschutzgesetze oder die SCC verlangen dies.

2.3 **Anbieter als eigenständiger Verantwortlicher.** Folgende personenbezogene Daten verarbeitet der Anbieter als eigenständiger Verantwortlicher und nicht nach dieser AVV, und zwar gemäß seiner Datenschutzerklärung (Privacy Notice, growmino.de/legal/privacy): (a) Konto- und Registrierungsdaten des Kunden und seiner Authorised Users (etwa Name, geschäftliche E-Mail-Adresse, Unternehmen, Rolle und Zugangsdaten); (b) Abrechnungs-, Zahlungs-, Steuer- und Vertragsverwaltungsdaten, einschließlich der unveränderlichen Protokolle über Vertragszustimmungen; (c) Daten, die für die Sicherheit, Integrität und Missbrauchsverhinderung der Services verarbeitet werden (etwa Authentifizierungsprotokolle, Rate-Limiting-Daten und Audit-Logs administrativer Aktionen), soweit diese zu eigenen Zwecken des Anbieters verarbeitet werden; und (d) Kommunikation zwischen Kunde und Anbieter (etwa Supportanfragen und rechtliche Mitteilungen).

2.4 **Stripe.** Die Zahlungsabwicklung erfolgt durch Stripe Payments Europe, Limited und Stripe, Inc. („Stripe“) als eigenständige Verantwortliche nach deren eigenen Bedingungen und Datenschutzerklärungen. Stripe ist kein Unterauftragsverarbeiter des Anbieters.

2.5 **Vom Kunden verbundene Dienste.** Vom Kunden verbundene Dienste sind Dienste des Kunden. Ihre Anbieter sind keine Unterauftragsverarbeiter des Anbieters. Der Kunde ist verantwortlich für seine Verträge mit diesen Anbietern, für die Rechtmäßigkeit der von ihm veranlassten Datenflüsse zwischen den Services und den vom Kunden verbundenen Diensten sowie für die Einstellungen in diesen Diensten. Daten, die der Anbieter von vom Kunden verbundenen Diensten empfängt oder an diese sendet, verarbeitet er als Auftragsverarbeiter des Kunden nach dieser AVV.

2.6 **Verantwortung des Kunden.** Der Kunde ist allein verantwortlich für (a) die Rechtmäßigkeit der Verarbeitung der Kunden-personenbezogenen Daten einschließlich des Vorliegens einer Rechtsgrundlage; (b) die Information der betroffenen Personen nach Art. 13 und 14 DSGVO; (c) die Einholung gesetzlich erforderlicher Einwilligungen, insbesondere für die Aufzeichnung von Telefongesprächen, für Werbung per E-Mail, SMS oder Telefon und für die Verarbeitung von Daten Minderjähriger; (d) die Einhaltung arbeitsrechtlicher und mitbestimmungsrechtlicher Vorgaben bei Nutzung des HR-Moduls, einschließlich einer etwaigen Beteiligung eines Betriebsrats; (e) die Richtigkeit und Qualität der Kunden-personenbezogenen Daten; und (f) dafür, besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO oder Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO nur einzugeben, soweit Datenschutzgesetze dies erlauben, und, soweit die Services dafür vorgesehene Felder bereitstellen, nur in diesen Feldern.

2.7 **Kein KI-Training.** Der Anbieter verwendet Kunden-personenbezogene Daten nicht zum Training von Modellen künstlicher Intelligenz und gestattet dies auch seinen Unterauftragsverarbeitern nicht.

---

3. Einzelheiten der Verarbeitung

3.1 Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1, getrennt für jedes Modul und für Professional Services.

3.2 Die Dauer der Verarbeitung entspricht der Laufzeit des Vertrags zuzüglich der in Abschnitt 10 geregelten Fristen für Export und Löschung.

---

4. Weisungen

4.1 **Dokumentierte Weisungen.** Der Anbieter verarbeitet Kunden-personenbezogene Daten nur auf dokumentierte Weisung des Kunden, auch in Bezug auf die Übermittlung an ein

Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten oder anderes Recht, dem der Anbieter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Anbieter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 **Was als Weisung gilt.** Die dokumentierten Weisungen des Kunden zum Inkrafttreten sind diese AVV und der Vertrag. Weitere Weisungen erteilt der Kunde (a) durch die Konfiguration und Nutzung der Services durch ihn und seine Authorised Users, einschließlich Einstellungen, Workflows, Automatisierungen, Integrationen, Importen, Exporten und Löschungen; und (b) in Textform per E-Mail an office@growmino.de. Weisungen, die über die Funktionalität und den Umfang des Vertrags hinausgehen, bedürfen einer gesonderten Vereinbarung, für die der Anbieter eine angemessene Vergütung verlangen kann.

4.3 **Rechtswidrige Weisungen.** Der Anbieter informiert den Kunden unverzüglich, wenn eine Weisung seiner Auffassung nach gegen die DSGVO oder andere Datenschutzgesetze verstößt. Der Anbieter darf die Ausführung der betreffenden Weisung aussetzen, bis der Kunde sie bestätigt oder ändert. Zu einer umfassenden rechtlichen Prüfung der Weisungen des Kunden ist der Anbieter nicht verpflichtet.

4.4 **Zweckbindung.** Der Anbieter verarbeitet Kunden-personenbezogene Daten zu keinem anderen Zweck als zur Bereitstellung, Wartung, Absicherung und Unterstützung der Services gemäß dem Vertrag und den Weisungen des Kunden.

---

5. Vertraulichkeit und Sicherheit

5.1 **Vertraulichkeit der Personen.** Der Anbieter gewährleistet, dass sich alle zur Verarbeitung der Kunden-personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Anbieter wird von einer Person betrieben. Eine Vertretung nach der Vertretungsregelung im Operating Agreement des Anbieters wird vor Erhalt des Zugriffs zur Vertraulichkeit verpflichtet. Die Vertraulichkeitspflicht gilt über das Ende der Tätigkeit hinaus fort.

5.2 **Zugriff durch den Anbieter.** Der Anbieter greift auf Kunden-personenbezogene Daten nur zu, soweit dies erforderlich ist, um vom Kunden angefragten Support zu leisten, Weisungen des Kunden auszuführen, die Sicherheit und den Betrieb der Services aufrechtzuerhalten oder gesetzliche Pflichten zu erfüllen.

5.3 **Sicherheitsmaßnahmen.** Der Anbieter trifft und unterhält die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Sinne von Art. 32 DSGVO zu gewährleisten, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

5.4 **Änderungen.** Die Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Anbieter darf sie durch gleichwertige alternative Maßnahmen ersetzen. Das Gesamtschutzniveau wird der Anbieter während der Vertragslaufzeit nicht absenken.

5.5 **Eigene Maßnahmen des Kunden.** Der Kunde ist für die Sicherheitsmaßnahmen in seinem Einflussbereich verantwortlich, insbesondere für die Nutzerverwaltung, die Vergabe von Rollen, die Aktivierung der Zwei-Faktor-Authentifizierung für seine Administratoren, soweit verfügbar, den Schutz seiner Zugangsdaten und API-Keys sowie die Sicherheit der vom Kunden verbundenen Dienste und seiner Geräte einschließlich Zeiterfassungsterminals.

---

6. Unterauftragsverarbeiter

6.1 **Allgemeine Genehmigung.** Der Kunde erteilt die allgemeine Genehmigung zur Beauftragung der auf growmino.de/legal/subprocessors aufgeführten Unterauftragsverarbeiter. Die Liste zum Inkrafttreten ist in Anlage 3 wiedergegeben.

6.2 **Ankündigung von Änderungen.** Der Anbieter kündigt jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage im Voraus per E-Mail und auf dieser Seite an. Administratoren des Kunden erhalten diese Mitteilungen automatisch. Andere Personen können sie per Anfrage an office@growmino.de abonnieren.

6.3 **Einspruch.** Der Kunde kann innerhalb von 30 Tagen nach der Ankündigung aus berechtigten datenschutzrechtlichen Gründen Einspruch erheben. Der Anbieter bemüht sich, eine zumutbare Alternative vorzuschlagen. Ist keine verfügbar, kann der Kunde die betroffenen Services mit Wirkung zum Zeitpunkt des Wirksamwerdens der Änderung kündigen und erhält eine anteilige Erstattung nach Abschnitt 10.3(c) der Terms. Da der Kunde nach Abschnitt 6.1 eine allgemeine Genehmigung erteilt hat, ist keine weitere Zustimmung erforderlich; erhebt der Kunde innerhalb der Ankündigungsfrist keinen Einspruch, erstreckt sich diese allgemeine Genehmigung auf den neuen Unterauftragsverarbeiter.

6.4 **Notfall-Ersetzung.** Ist eine sofortige Ersetzung erforderlich, um die Sicherheit oder Verfügbarkeit der Services aufrechtzuerhalten, darf der Anbieter einen Unterauftragsverarbeiter ohne vorherige Ankündigung ersetzen und informiert den Kunden unverzüglich; Abschnitt 6.3 gilt entsprechend.

6.5 **Weitergabe der Pflichten und Haftung.** Der Anbieter erlegt jedem Unterauftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht eines Mitgliedstaats Datenschutzpflichten auf, die denen dieser AVV gleichwertig sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht, einschließlich geeigneter Garantien für Übermittlungen nach Kapitel V DSGVO. Der Anbieter haftet dem Kunden gegenüber in vollem Umfang für die Einhaltung der Pflichten seiner Unterauftragsverarbeiter. Bietet ein Unterauftragsverarbeiter nur

Standardbedingungen an, sind sich die Parteien einig, dass diese Bedingungen Abschnitt 6.5 genügen, wenn sie die Anforderungen von Art. 28 Abs. 3 und 4 DSGVO erfüllen.

6.6 **Kopien.** Auf Anfrage stellt der Anbieter dem Kunden Informationen über die mit einem Unterauftragsverarbeiter vereinbarten Datenschutzbedingungen zur Verfügung. Kaufmännische Informationen und vertrauliche Bedingungen darf der Anbieter entfernen oder schwärzen.

---

7. Unterstützung

7.1 **Anträge betroffener Personen.** Angesichts der Art der Verarbeitung unterstützt der Anbieter den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen. Die Services bieten Funktionen zum Suchen, Anzeigen, Berichtigen, Exportieren und Löschen von Kunden-personenbezogenen Daten. Kann der Kunde einen Antrag mit diesen Funktionen nicht erfüllen, leistet der Anbieter auf Anfrage angemessene weitere Unterstützung.

7.2 **Beim Anbieter eingehende Anträge.** Richtet eine betroffene Person einen Antrag zu Kunden-personenbezogenen Daten unmittelbar an den Anbieter, leitet der Anbieter ihn unverzüglich an den Kunden weiter, soweit er den Kunden identifizieren kann, und beantwortet den Antrag nicht selbst, es sei denn, der Kunde hat ihn hierzu ermächtigt oder das Gesetz verlangt dies.

7.3 **Sicherheit, Datenpannen, DSFA und vorherige Konsultation.** Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Anbieter den Kunden bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere durch Informationen über die Services und die Maßnahmen in Anlage 2 für Datenschutz-Folgenabschätzungen des Kunden und, soweit erforderlich, für vorherige Konsultationen der Aufsichtsbehörde.

7.4 **Behörden.** Der Anbieter arbeitet auf Anfrage mit der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen und informiert den Kunden unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, die Kunden-personenbezogene Daten betreffen, soweit dies rechtlich zulässig ist.

7.5 **Verzeichnis.** Der Anbieter führt ein Verzeichnis zu allen Kategorien von im Auftrag des Kunden durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 DSGVO, soweit diese Pflicht für ihn gilt.

7.6 **Kosten.** Unterstützung nach diesem Abschnitt 7 ist unentgeltlich, soweit sie über die Funktionen der Services erfolgt oder eine Verletzung des Schutzes personenbezogener Daten im Verantwortungsbereich des Anbieters betrifft. Für sonstige Unterstützung mit erheblichem Aufwand kann der Anbieter nach vorheriger Information des Kunden eine angemessene Vergütung zu seinen jeweils aktuellen Sätzen verlangen.

8. Verletzung des Schutzes personenbezogener Daten

8.1 Der Anbieter benachrichtigt den Kunden unverzüglich und, soweit möglich, innerhalb von 48 Stunden, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die Kundendaten betrifft. Die Meldung enthält, soweit bekannt, die nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen; weitere Informationen stellt der Anbieter schrittweise zur Verfügung, sobald sie vorliegen.

8.2 Der Anbieter ergreift angemessene Maßnahmen, um die Verletzung einzudämmen und zu beheben, und unterstützt den Kunden bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

8.3 Der Anbieter sendet Meldungen an die im Konto hinterlegten E-Mail-Adressen der Administratoren des Kunden und, sofern der Kunde einen benannt hat, an dessen Datenschutzkontakt. Der Kunde ist dafür verantwortlich, diese Adressen aktuell zu halten.

8.4 Der Anbieter dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich der Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen.

8.5 Die Meldung des Anbieters ist kein Anerkenntnis eines Verschuldens oder einer Haftung.

9. Informationen und Audits

9.1 **Informationen.** Der Anbieter stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO und dieser AVV niedergelegten Pflichten zur Verfügung. Diese Pflicht erfüllt der Anbieter vorrangig durch Dokumente, insbesondere diese AVV mit Anlagen, die unter growmino.de/legal/security veröffentlichten Security & Data Act Information, schriftliche Antworten auf angemessene Sicherheitsfragebögen sowie, soweit verfügbar und weitergabefähig, Zertifizierungen oder Prüfberichte seiner Unterauftragsverarbeiter.

9.2 **Audits.** Reichen die nach Abschnitt 9.1 bereitgestellten Dokumente zum Nachweis nicht aus, kann der Kunde auf eigene Kosten eine Überprüfung durchführen oder durch einen zur Verschwiegenheit verpflichteten unabhängigen Prüfer durchführen lassen, höchstens einmal in einem Zeitraum von 12 Monaten und mit einer Vorankündigung von mindestens 30 Tagen in Textform. Audits erfolgen remote oder, soweit erforderlich, in den Geschäftsräumen des Anbieters während der üblichen Geschäftszeiten (MEZ), ohne unzumutbare Störung des Betriebs des Anbieters und ohne Zugang zu Daten anderer Kunden oder zu vertraulichen Informationen des Anbieters, die nicht mit der Verarbeitung der Kunden-personenbezogenen Daten zusammenhängen. Der Anbieter kann einem Prüfer widersprechen, der Wettbewerber des Anbieters ist.

9.3 **Zusätzliche Audits.** Unabhängig von der Häufigkeitsgrenze in Abschnitt 9.2 kann der Kunde ein zusätzliches Audit durchführen, (a) nach einer Verletzung des Schutzes

personenbezogener Daten, die Kunden-personenbezogene Daten betrifft, oder (b) wenn eine zuständige Aufsichtsbehörde dies verlangt oder anordnet.

9.4 **Einrichtungen der Unterauftragsverarbeiter.** Der Anbieter betreibt für die Services keine eigenen Rechenzentren. Die Überprüfung von Rechenzentrums- und Infrastrukturmaßnahmen erfolgt über die Zertifizierungen, Berichte und Prüfmechanismen, die die Unterauftragsverarbeiter bereitstellen.

9.5 **SCC.** Klausel 8.9 der SCC bleibt unberührt. Die Abschnitte 9.1 bis 9.4 beschreiben, wie der Anbieter sie umsetzt.

---

10. Rückgabe und Löschung

10.1 **Export.** Während der Vertragslaufzeit kann der Kunde Kundendaten jederzeit mit den Exportfunktionen der Services exportieren. Nach Kündigung oder Ablauf des Vertrags oder nach dem Ende einer Testphase ohne Wahl eines kostenpflichtigen Plans kann der Kunde Kundendaten nach den Zugangsstufen in Abschnitt 10.9 der Terms 90 Tage lang exportieren. Die Wechsel- und Exit-Regeln in Schedule 4 der Terms bleiben unberührt und gehen vor, soweit sie längere Fristen vorsehen.

10.2 **Löschung.** Nach Ablauf der Exportfrist löscht der Anbieter die Kunden-personenbezogenen Daten innerhalb von 30 Tagen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder anderem Recht, dem der Anbieter unterliegt, eine Verpflichtung zur Speicherung besteht. Kopien in Backups werden im regulären Backup-Zyklus innerhalb von 90 Tagen gelöscht. Bis zu ihrer Löschung werden Backups unter den Maßnahmen der Anlage 2 aufbewahrt und zu keinem anderen Zweck verwendet.

10.3 **Frühere Löschung.** Der Kunde kann Kunden-personenbezogene Daten jederzeit mit den Funktionen der Services löschen oder den Anbieter per E-Mail anweisen, sie früher zu löschen. Für Backups gilt Abschnitt 10.2.

10.4 **Gesetzliche Aufbewahrung.** Muss der Anbieter Kunden-personenbezogene Daten von Gesetzes wegen aufbewahren, schränkt er ihre Verarbeitung auf die Zwecke dieser Aufbewahrung ein und löscht sie nach Ablauf der Aufbewahrungsfrist.

10.5 **Bestätigung.** Auf Anfrage bestätigt der Anbieter dem Kunden die Löschung in Textform.

---

11. Internationale Übermittlungen und Standardvertragsklauseln

11.1 **Sitz des Anbieters.** Der Anbieter hat seinen Sitz in den USA. Kunden-personenbezogene Daten werden in den in Anlage 1 und Anlage 3 genannten Regionen gehostet. Fernzugriffe

durch den Anbieter und bestimmte Unterauftragsverarbeiter aus Drittländern sind möglich.

11.2 **Einbeziehung der SCC.** Soweit die Verarbeitung eine Übermittlung personenbezogener Daten in ein Drittland umfasst, die Kapitel V DSGVO unterliegt, und kein anderer Übermittlungsmechanismus (insbesondere ein Angemessenheitsbeschluss einschließlich des EU-U.S. Data Privacy Framework) greift, werden die SCC durch Verweis in diese AVV einbezogen: Modul 2 (Verantwortlicher an Auftragsverarbeiter), soweit der Kunde Verantwortlicher ist, und Modul 3 (Auftragsverarbeiter an Auftragsverarbeiter), soweit der Kunde Auftragsverarbeiter ist. Der Kunde ist Datenexporteur, der Anbieter Datenimporteur. Solange der Anbieter nicht nach dem DPF zertifiziert ist und dies dem Kunden mitgeteilt hat, beruhen Übermittlungen vom Kunden an den Anbieter auf den SCC.

11.3 **Optionen.** Für die SCC gelten folgende Optionen:

- Klausel 7 (Kopplungsklausel) gilt.
- Klausel 9(a): Option 2 (allgemeine schriftliche Genehmigung) gilt mit einer Frist von 30 Tagen. Für das Verfahren gilt Abschnitt 6 dieser AVV.
- Klausel 11(a): Die optionale Formulierung gilt nicht.
- Klausel 13: (a) ist der Kunde in der EU niedergelassen, die Aufsichtsbehörde seiner Niederlassung; (b) ist der Kunde nicht in der EU niedergelassen, hat er aber einen Vertreter nach Art. 27 DSGVO benannt, die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter niedergelassen ist; (c) andernfalls die Aufsichtsbehörde des Mitgliedstaats, in dem sich die betroffenen Personen befinden, deren personenbezogene Daten übermittelt werden.
- Klausel 17: Option 1 gilt; die SCC unterliegen dem Recht der Bundesrepublik Deutschland.
- Klausel 18(b): Streitigkeiten werden von den Gerichten in Deutschland entschieden.

11.4 **Anhänge.** Anhang I.A: Datenexporteur ist der Kunde, wie in seinem Konto, Order Form oder SOW bezeichnet, mit den dort hinterlegten Kontaktdaten; seine Tätigkeit ist die Nutzung der Services im Rahmen des Vertrags; Datenimporteur ist der Anbieter mit den zu Beginn dieser AVV genannten Angaben, tätig als Auftragsverarbeiter (Modul 2) oder Unterauftragsverarbeiter (Modul 3); die Annahme der Terms durch die Parteien gilt als Unterzeichnung von Anhang I.A. Anhang I.B: Anlage 1, je Modul. Anhang I.C: die nach Klausel 13 gemäß Abschnitt 11.3 bestimmte zuständige Aufsichtsbehörde. Anhang II: Anlage 2. Anhang III: Anlage 3 und die Liste unter growmino.de/legal/subprocessors.

11.5 **Transfer Impact Assessment.** Der Anbieter hat die für ihn und seine Unterauftragsverarbeiter geltenden Rechtsvorschriften und Gepflogenheiten der USA gemäß Klausel 14 der SCC beurteilt und stellt dem Kunden auf Anfrage die für dessen eigene Beurteilung vernünftigerweise erforderlichen Informationen zur Verfügung. Der Anbieter informiert den Kunden unverzüglich, wenn er Grund zu der Annahme hat, dass er Rechtsvorschriften oder Gepflogenheiten unterliegt oder unterworfen wurde, die nicht mit den Anforderungen von Klausel 14(a) der SCC im Einklang stehen.

11.6 **Weiterübermittlungen.** Der Anbieter übermittelt Kunden-personenbezogene Daten an Unterauftragsverarbeiter in Drittländern, insbesondere an in den USA ansässige Unterauftragsverarbeiter, nur auf Grundlage (a) der DPF-Zertifizierung des jeweiligen

Unterauftragsverarbeiters, soweit vorhanden und die Verarbeitung abdeckend, oder (b) mit dem Unterauftragsverarbeiter geschlossener Standardvertragsklauseln (Modul 3, Auftragsverarbeiter an Auftragsverarbeiter) oder (c) einer anderen geeigneten Garantie nach Art. 46 DSGVO. Damit werden Klausel 8.7 und Klausel 9 der SCC umgesetzt. Der Anbieter stützt sich auf die SCC und, soweit vorhanden, auf die DPF-Zertifizierung der Unterauftragsverarbeiter. Der Anbieter beansprucht keine eigene DPF-Zertifizierung.

11.7 **Vereinigtes Königreich.** Für Beschränkte Übermittlungen, die der UK GDPR unterliegen, wird das UK Addendum durch Verweis einbezogen und gilt wie folgt: Tabelle 1 wird mit den Angaben in Abschnitt 11.4 (Anhang I.A) ausgefüllt; Tabelle 2 mit den in Abschnitt 11.3 gewählten Modulen und Optionen; Tabelle 3 mit Anlage 1, Anlage 2 und Anlage 3; in Tabelle 4 darf keine Partei das UK Addendum nach dessen Section 19 beenden. Soweit für einen Unterauftragsverarbeiter die UK-Erweiterung des DPF gilt, kann sie für Weiterübermittlungen herangezogen werden.

11.8 **Schweiz.** Für Beschränkte Übermittlungen, die dem DSG unterliegen, gelten die SCC mit folgenden Anpassungen: Verweise auf die DSGVO gelten als Verweise auf das DSG; zuständige Aufsichtsbehörde ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB); betroffene Personen in der Schweiz können ihre Ansprüche in der Schweiz geltend machen; und der Begriff „Mitgliedstaat“ schließt die Schweiz ein, sodass betroffene Personen mit gewöhnlichem Aufenthalt in der Schweiz nicht von der Klagemöglichkeit an ihrem gewöhnlichen Aufenthaltsort ausgeschlossen sind.

11.9 **Andere Rechtsordnungen.** Verlangen andere Datenschutzgesetze einen bestimmten Übermittlungsmechanismus, wirken die Parteien nach Treu und Glauben an dessen Umsetzung mit. Bis dahin gelten die SCC entsprechend, soweit zulässig.

11.10 **Hinweis zu Erwägungsgrund 7.** Soweit der Anbieter für einen bestimmten Verarbeitungsvorgang selbst nach Art. 3 Abs. 2 DSGVO der DSGVO unterliegt, gelten die SCC nur in dem nach Kapitel V DSGVO erforderlichen Umfang.

11.11 **Vorrang der SCC.** Bei Widersprüchen zwischen den SCC und dieser AVV oder den Terms gehen die SCC vor. Nichts im Vertrag soll den SCC direkt oder indirekt widersprechen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beeinträchtigen.

---

12. Zugriffsersuchen von Behörden

12.1 **Benachrichtigung.** Der Anbieter benachrichtigt den Kunden und, soweit möglich, die betroffene Person unverzüglich, wenn er (a) von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes oder eines anderen Drittlandes rechtlich bindendes Ersuchen um Offenlegung von Kunden-personenbezogenen Daten erhält; oder (b) Kenntnis davon erlangt, dass Behörden direkt auf Kunden-personenbezogene Daten zugegriffen haben. Die Benachrichtigung enthält Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die erteilte Antwort.

12.2 **Benachrichtigungsverbot.** Ist es dem Anbieter untersagt, den Kunden zu benachrichtigen, bemüht er sich nach besten Kräften um eine Aufhebung des Verbots, um möglichst viele Informationen so schnell wie möglich mitteilen zu können. Der Anbieter dokumentiert seine Bemühungen, um sie auf Verlangen nachweisen zu können.

12.3 **Prüfung und Anfechtung.** Der Anbieter prüft die Rechtmäßigkeit jedes Offenlegungsersuchens, insbesondere ob es im Rahmen der Befugnisse der ersuchenden Behörde bleibt, und ficht das Ersuchen an, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe für die Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, den geltenden völkerrechtlichen Verpflichtungen und den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter denselben Bedingungen schöpft der Anbieter Rechtsmittel aus. Bei der Anfechtung eines Ersuchens erwirkt der Anbieter einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über die Begründetheit entschieden hat. Der Anbieter legt die angeforderten personenbezogenen Daten erst offen, wenn er nach den geltenden Verfahrensregeln dazu verpflichtet ist.

12.4 **Datenminimierung.** Bei der Beantwortung eines Ersuchens stellt der Anbieter auf Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereit.

12.5 **Transparenz.** Der Anbieter stellt dem Kunden in regelmäßigen Abständen und auf Anfrage so viele einschlägige Informationen wie möglich über die eingegangenen Ersuchen zur Verfügung, insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörden, ob Ersuchen angefochten wurden und mit welchem Ergebnis, soweit rechtlich zulässig. Der Anbieter bewahrt die Dokumentation seiner rechtlichen Beurteilung und etwaiger Anfechtungen für die Dauer des Vertrags auf und stellt sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung.

12.6 **Keine Hintertüren.** Der Anbieter hat keine Hintertüren oder ähnliche Programmierungen geschaffen, die für den Zugriff auf die Services oder auf Kunden-personenbezogene Daten genutzt werden könnten, und ist weder rechtlich noch faktisch verpflichtet, solche zu schaffen oder aufrechtzuerhalten.

12.7 Dieser Abschnitt 12 entspricht Klausel 15 der SCC und gilt unabhängig davon, ob die SCC anwendbar sind. Soweit die SCC anwendbar sind, geht Klausel 15 der SCC vor.

---

13. EU-Vertreter

13.1 Der Anbieter hat gemäß Art. 27 DSGVO folgenden Vertreter in der Union benannt: David Wolff, Einzelunternehmen, Grüne Gärtel 7, 76316 Malsch, Deutschland, office@growmino.de.

13.2 Aufsichtsbehörden und betroffene Personen können sich zusätzlich zum Anbieter oder an seiner Stelle in allen Fragen im Zusammenhang mit der Verarbeitung an den Vertreter wenden. Der Vertreter ist beauftragt, das Verzeichnis von Verarbeitungstätigkeiten zu führen.

13.3 Einen Datenschutzbeauftragten hat der Anbieter nicht benannt, da er hierzu nach Art. 37 DSGVO nicht verpflichtet ist.

---

14. Haftung

14.1 Die Haftung jeder Partei aus oder im Zusammenhang mit dieser AVV unterliegt den Haftungsbeschränkungen und -ausschlüssen in Abschnitt 15 der Terms, einschließlich des Data Cap, soweit nach anwendbarem Recht zulässig.

14.2 Nichts in dieser AVV oder in den Terms beschränkt oder schließt aus: (a) die Haftung einer Partei gegenüber betroffenen Personen, einschließlich nach Art. 82 DSGVO und Klausel 12(b) und (c) der SCC; (b) die Haftung gegenüber einer Aufsichtsbehörde für gegen diese Partei verhängte Geldbußen; oder (c) eine Haftung, die nach zwingendem anwendbarem Recht nicht beschränkt werden kann. Die interne Haftungsverteilung zwischen den Parteien nach Art. 82 Abs. 5 DSGVO bleibt unberührt.

---

15. US-Bundesstaaten-Datenschutzgesetze

Soweit der CCPA oder andere US-Bundesstaaten-Datenschutzgesetze anwendbar sind, handelt der Anbieter als „Service Provider“ bzw. „Processor“ des Kunden und (a) verkauft oder teilt („sell“ bzw. „share“ im Sinne des CCPA) Kunden-personenbezogene Daten nicht; (b) speichert, verwendet oder offenbart Kunden-personenbezogene Daten zu keinem anderen Zweck, einschließlich kommerzieller Zwecke, als den im Vertrag festgelegten Geschäftszwecken und nicht außerhalb der unmittelbaren Geschäftsbeziehung mit dem Kunden; (c) kombiniert Kunden-personenbezogene Daten nicht mit personenbezogenen Daten aus anderen Quellen, außer soweit nach dem CCPA zulässig; (d) hält den CCPA ein und gewährleistet dasselbe Datenschutzniveau, das der CCPA von Unternehmen verlangt; (e) teilt dem Kunden mit, wenn er feststellt, dass er diese Pflichten nicht mehr erfüllen kann; und (f) gestattet dem Kunden, angemessene und geeignete Schritte zu unternehmen, um eine unbefugte Nutzung von Kunden-personenbezogenen Daten zu unterbinden und zu beheben. Der Anbieter bestätigt, dass er diese Beschränkungen versteht und einhalten wird.

---

16. Laufzeit

16.1 Diese AVV tritt mit Annahme der Terms in Kraft und gilt, solange der Anbieter Kunden-personenbezogene Daten verarbeitet, unabhängig von der Beendigung des Vertrags.

16.2 Bestimmungen, die ihrer Natur nach über das Ende der Verarbeitung hinaus fortgelten sollen, insbesondere die Abschnitte 5.1, 10, 12 und 14, gelten nach Beendigung fort.

---

17. Rangfolge und allgemeine Bestimmungen

17.1 **Rangfolge.** Für die Verarbeitung personenbezogener Daten gilt folgende Rangfolge: (1) die SCC mit ihren Anhängen, soweit anwendbar; (2) diese AVV; (3) die Terms und die übrigen Vertragsbestandteile. Ein Order Form oder SOW geht dieser AVV nur vor, soweit es ausdrücklich bestimmt, dass es von ihr abweicht, und die Abweichung nach den Datenschutzgesetzen zulässig ist.

17.2 **Anwendbares Recht und Streitigkeiten.** Mit Ausnahme der SCC (Abschnitt 11.3 sowie Klauseln 17 und 18 der SCC) und soweit Datenschutzgesetze nicht zwingend etwas anderes vorschreiben, unterliegt diese AVV den Bestimmungen der Terms zu anwendbarem Recht und Streitbeilegung.

17.3 **Änderungen.** Der Anbieter kann diese AVV nach dem Verfahren für Änderungen der Terms ändern. Schweigen oder fortgesetzte Nutzung gilt nicht als Zustimmung zu wesentlichen oder nachteiligen Änderungen. Anlage 3 kann der Anbieter nach Abschnitt 6 aktualisieren. Änderungen, die durch eine Änderung der Datenschutzgesetze oder durch eine Entscheidung einer zuständigen Behörde oder eines Gerichts erforderlich werden, können mit der in den Terms genannten Ankündigungsfrist umgesetzt werden.

17.4 **Salvatorische Klausel.** Ist eine Bestimmung dieser AVV unwirksam oder undurchsetzbar, bleiben die übrigen Bestimmungen wirksam. An die Stelle der unwirksamen Bestimmung tritt eine wirksame Bestimmung, die dem beabsichtigten Zweck möglichst nahekommt, und in jedem Fall die Anforderungen von Art. 28 Abs. 3 DSGVO.

17.5 **Sprache.** Diese AVV wird in englischer Sprache geschlossen. Übersetzungen dienen nur der Information. Bei Widersprüchen geht die englische Fassung vor, soweit zwingendes Recht nichts anderes verlangt.

Anlage 1: Einzelheiten der Verarbeitung (Anhang I der SCC)

A. Liste der Parteien (Anhang I.A)

Datenexporteur: der Kunde mit Name, Anschrift und Kontaktdaten gemäß seinem Konto, Order Form oder SOW. Für die übermittelten Daten relevante Tätigkeiten: Nutzung der Growmino-One-Services und, soweit vereinbart, der Professional Services im Rahmen des Vertrags. Rolle: Verantwortlicher (Modul 2) oder Auftragsverarbeiter (Modul 3). Unterschrift

und Datum: Annahme der Terms in der Anwendung oder Unterzeichnung des Order Form bzw. SOW.

Datenimporteur: PUSH - CONSULTING LLC, 30 N Gould St Ste N, Sheridan, WY 82801, USA, Wyoming Secretary of State Filing ID 2026-002106936. Kontakt: David Wolff, Sole Member und Manager, office@growmino.de, +49 176 31685433. EU-Vertreter nach Art. 27 DSGVO: David Wolff, Einzelunternehmen, Grüne Gärtel 7, 76316 Malsch, Deutschland, office@growmino.de. Für die übermittelten Daten relevante Tätigkeiten: Bereitstellung, Hosting, Betrieb, Support und Sicherheit der Services sowie Erbringung von Professional Services. Rolle: Auftragsverarbeiter (Modul 2) oder Unterauftragsverarbeiter (Modul 3). Unterschrift und Datum: Annahme der Terms durch den Kunden, die der Anbieter durch Bereitstellung der Services bestätigt.

B. Beschreibung der Übermittlung und Verarbeitung (Anhang I.B)

Für alle Module gilt, soweit nicht anders angegeben:

- **Art der Verarbeitung:** Erhebung über die Services und Schnittstellen, Speicherung, Organisation, Ordnen, Abfragen, Auslesen, Verwendung, Abgleich und Verknüpfung entsprechend der Konfiguration durch den Kunden, Übermittlung an vom Kunden gewählte Empfänger, Einschränkung, Export und Löschung.
- **Häufigkeit der Übermittlung:** fortlaufend für die Dauer des Vertrags.
- **Speicherdauer:** wie vom Kunden durch seine Nutzung der Services bestimmt; spätestens bis zur Löschung nach Abschnitt 10 der AVV (90 Tage Exportfenster nach Ende des Vertrags oder Abonnements, Löschung innerhalb weiterer 30 Tage, Backups innerhalb von 90 Tagen).
- **Nutzer aller Module:** Authorised Users des Kunden (Beschäftigte, Auftragnehmer und andere vom Kunden befugte Personen). Ihre Profildaten, Rollen, Berechtigungen, Aktivitäten und Audit-Einträge innerhalb der Organisation des Kunden werden im Auftrag des Kunden verarbeitet, unbeschadet Abschnitt 2.3 der AVV.
- **Hosting und Übermittlungen an Unterauftragsverarbeiter:** siehe jeweiliges Modul und Anlage 3. Alle Module werden über Lovable (App-Hosting, Build, Transaktions-E-Mails über notify.growmino.de, AI Gateway) und Cloudflare (CDN und Edge-Ausführung weltweit) bereitgestellt. Bei der Edge-Verarbeitung werden Daten während der Übertragung verarbeitet; sie ist nicht der primäre Speicherort.

B.1 Growmino One CRM

- **Gegenstand und Zweck:** Verwaltung der Leads, Kontakte, Unternehmen, Deals und Vertriebspipeline des Kunden; E-Mail-Kommunikation und -Automatisierung; Kalendersynchronisation; Telefonie und SMS; KI-Transkription und -Zusammenfassung von Anrufen; Dashboards und KPIs; Listen; API, Webhooks, Import und Export.
- **Kategorien betroffener Personen:** Leads, Interessenten, Kunden des Kunden und deren Ansprechpartner; Geschäftspartner; Personen, die den Kunden per Telefon, SMS, E-Mail oder Webformular kontaktieren; Empfänger von Kommunikation des Kunden; Authorised Users.

- **Kategorien personenbezogener Daten:** Identitäts- und Kontaktdaten (Name, Titel, Unternehmen, Position, E-Mail-Adresse, Telefonnummer, Postanschrift); Pipeline- und Deal-Daten (Status, Wert, Produkte, Phase, Verantwortlicher); Notizen, Aufgaben, Anhänge und benutzerdefinierte Felder; Herkunfts- und Kampagnendaten aus Webhooks oder Importen (etwa Antworten aus Lead-Formularen); Inhalte und Metadaten von E-Mails, die über vom Kunden verbundene Dienste gesendet oder empfangen werden; Kalendereinträge; Anruf-Metadaten (Rufnummern, Zeitpunkt, Dauer, Richtung, Ergebnis); Sprachdaten, nämlich Anrufaufzeichnungen und Voicemails; Transkripte und KI-generierte Zusammenfassungen von Anrufen; SMS-Inhalte und -Metadaten; Kommunikationshistorie und vom Kunden erfasster Einwilligungsstatus.
- **Besondere Kategorien:** nicht vorgesehen. Offenbaren betroffene Personen in Anrufen, Nachrichten oder Notizen besondere Kategorien personenbezogener Daten, werden diese nur als Teil des jeweiligen Inhalts verarbeitet. Sprachaufzeichnungen werden nicht zur eindeutigen Identifizierung einer natürlichen Person verarbeitet.
- **Verarbeitungsort:** Datenbank, Authentifizierung und Speicher bei Supabase auf AWS eu-central-1 (Frankfurt, Deutschland).
- **Übermittlungen an Unterauftragsverarbeiter:** Supabase (Hosting); Lovable und Cloudflare (App-Auslieferung, E-Mail); Twilio (Telefonie, SMS, Aufzeichnungen, USA), soweit der Kunde die Telefonie des Anbieters nutzt; Google über das Lovable AI Gateway (Transkription und Zusammenfassungen), soweit der Kunde KI-Funktionen nutzt.

B.2 Growmino One Booking

- **Gegenstand und Zweck:** Erstellung und Verwaltung von Angeboten, Buchungen und Verträgen des Kunden mit seinen Endkunden; elektronische Signatur mit Audit-Trail per Link und Einmalpasswort (OTP); Rechnungsstellung des Kunden an seine Endkunden (PDF, ZUGFeRD); KI-gestützte Erstellung von Angeboten und Texten; Dokumentenbibliothek.
- **Kategorien betroffener Personen:** Endkunden des Kunden und deren Ansprechpartner; in Buchungen genannte Teilnehmende; Unterzeichnende; Authorised Users.
- **Kategorien personenbezogener Daten:** Identitäts- und Kontaktdaten (Name, Unternehmen, Postanschrift, E-Mail-Adresse, Telefonnummer); Buchungs- und Vertragsdaten (Leistungen, Termine, Preise, Teilnehmende, Vertragsinhalt, Anhänge und hochgeladene Dokumente); Signaturdaten (Name des Unterzeichnenden, Signaturbild oder getippte Signatur, für den Signaturlink verwendete E-Mail-Adresse, OTP-Verifizierungsereignisse, IP-Adresse, User-Agent, Zeitstempel und Audit-Trail-Einträge); Rechnungsdaten (Positionen, Beträge, Zahlungsstatus, vom Kunden angegebene Steuerangaben); Kommunikationsdaten zu Buchungen.
- **Besondere Kategorien:** nicht vorgesehen. Der Kunde darf besondere Kategorien personenbezogener Daten nur in Verträge oder Dokumente aufnehmen, soweit Datenschutzgesetze dies erlauben.
- **Verarbeitungsort:** Datenbank, Authentifizierung und Speicher bei Supabase auf AWS eu-west-1 (Irland).
- **Übermittlungen an Unterauftragsverarbeiter:** Supabase (Hosting); Lovable und Cloudflare (App-Auslieferung, E-Mail einschließlich Signaturlinks und OTP); Google über

das Lovable AI Gateway, soweit der Kunde KI-Credits nutzt.

B.3 Growmino One HR

- **Gegenstand und Zweck:** Zeiterfassung (einschließlich Terminal mit PIN und Offline-Modus), Abwesenheitsverwaltung, Dienstplanung, Arbeitszeitkonten, Ablage von Lohndokumenten, DATEV-Export, Standortverwaltung und REST-API (Enterprise).
- **Kategorien betroffener Personen:** Beschäftigte, Auszubildende, Leiharbeitnehmende und freie Mitarbeitende des Kunden; Führungskräfte und HR-Administratoren des Kunden; Authorised Users.
- **Kategorien personenbezogener Daten:** Identitäts- und Beschäftigungsdaten (Name, Personalnummer, Standort, Abteilung, Rolle, Vertragsart, Arbeitszeitmodell); Kontaktdaten; Arbeitszeitdaten (Kommen- und Gehen-Zeiten, Pausen, Terminal- und Gerätekennungen, Standortzuordnung, Offline-Einträge, Korrekturen und Freigaben); Arbeitszeitkonten und Dienstpläne; Abwesenheitsdaten (Art, Zeitraum, Status und, soweit vom Kunden erfasst, Abwesenheitsgrund); vom Kunden hochgeladene Lohndokumente (die Gehaltsdaten, Steuer- und Sozialversicherungskennungen und Bankverbindungen enthalten können); DATEV-Exportdaten; gehashte Terminal-PINs und API-Key-Hashes; Audit-Einträge.
- **Besondere Kategorien:** Abwesenheitsgründe können Gesundheitsdaten offenbaren (etwa Arbeitsunfähigkeit), und Lohndokumente können Daten enthalten, aus denen die Religionszugehörigkeit hervorgeht (etwa Kirchensteuerangaben). Schutzmaßnahmen: Der Kunde erfasst nur die für den jeweiligen Zweck erforderlichen Angaben (bei Arbeitsunfähigkeit grundsätzlich nur Tatsache und Dauer, keine Diagnose); der Zugriff ist durch das Rollen- und Rechtekonzept der Organisation beschränkt; Zwei-Faktor-Authentifizierung ist für HR-Administratoren Pflicht; Verschlüsselung bei der Übertragung und im Ruhezustand; Audit-Logs für administrative Aktionen.
- **Verarbeitungsort:** Datenbank, Authentifizierung und Speicher bei Supabase auf AWS eu-central-1 (Frankfurt, Deutschland).
- **Übermittlungen an Unterauftragsverarbeiter:** Supabase (Hosting); Lovable und Cloudflare (App-Auslieferung, E-Mail).

B.4 Growmino One Members (sobald verfügbar)

- **Gegenstand und Zweck:** Mitgliederverwaltung für Sportschulen, Clubs und Vereine, einschließlich Mitgliederdaten, Verträgen, Anwesenheit und Kommunikation. Dieser Abschnitt gilt ab dem Zeitpunkt, zu dem das Modul dem Kunden zur Verfügung gestellt wird.
- **Kategorien betroffener Personen:** Mitglieder und Interessenten, einschließlich Minderjähriger; Eltern und gesetzliche Vertreter; Trainer und Personal; Authorised Users.
- **Kategorien personenbezogener Daten:** Identitäts- und Kontaktdaten (Name, Geburtsdatum, Postanschrift, E-Mail-Adresse, Telefonnummer); Daten der Eltern oder gesetzlichen Vertreter; Mitgliedschafts- und Vertragsdaten (Tarif, Beginn und Ende, Status, Graduierungen oder Stufen); Anwesenheits- und Check-in-Daten; Kommunikationsdaten; Fotos, soweit vom Kunden hochgeladen.

- **Besondere Kategorien:** Gesundheitsdaten nur in den dafür vorgesehenen Feldern und erst nach Durchführung einer Datenschutz-Folgenabschätzung für das Modul. Schutzmaßnahmen: nur vorgesehene Felder; Zugriffsbeschränkung durch das Rollen- und Rechtekonzept; Verschlüsselung bei der Übertragung und im Ruhezustand; Audit-Logs für administrative Aktionen. Der Kunde ist für die Rechtsgrundlage einschließlich etwaiger ausdrücklicher Einwilligungen sowie für erforderliche Einwilligungen der Eltern oder gesetzlichen Vertreter bei Minderjährigen verantwortlich.
- **Verarbeitungsort und Übermittlungen an Unterauftragsverarbeiter:** wie in Anlage 3 zum Zeitpunkt der Bereitstellung des Moduls angegeben. Der Anbieter kündigt die Hosting-Region nach Abschnitt 6 der AVV an.

B.5 Professional Services

- **Gegenstand und Zweck:** Entwicklung von Websites und Webanwendungen, KI-Automatisierung, Betreuung von Google- und Meta-Werbung, Content- und KI-Videoproduktion sowie Beratung, jeweils wie im SOW beschrieben und soweit der Anbieter dabei Kunden-personenbezogene Daten verarbeitet.
- **Kategorien betroffener Personen:** wie im SOW festgelegt, typischerweise Website-Besucher, Leads und Kunden des Kunden, Empfänger von Werbung, Personen, die in vom Kunden bereitgestellten Inhalten zu sehen oder zu hören sind, sowie Beschäftigte und Ansprechpartner des Kunden.
- **Kategorien personenbezogener Daten:** wie im SOW festgelegt, typischerweise Kontakt- und Formulardaten, Lead-Daten, Daten zu Werbezielgruppen in den Werbekonten des Kunden, Nutzungsdaten von für den Kunden betriebenen Websites sowie vom Kunden bereitgestellte Bilder, Videos und Sprachaufnahmen.
- **Verarbeitungsort und Übermittlungen an Unterauftragsverarbeiter:** die in Anlage 3 für den jeweiligen Dienst genannten Unterauftragsverarbeiter sowie im SOW zusätzlich benannte Unterauftragsverarbeiter. Eigene Werbe-, Analyse- und Integrationskonten des Kunden sind vom Kunden verbundene Dienste. Vom Kunden bereitgestellte Bilder, Videos oder Sprachaufnahmen identifizierbarer Personen lädt der Anbieter nicht in generative KI-Dienste hoch, es sei denn, das SOW sieht dies ausdrücklich vor.

C. Zuständige Aufsichtsbehörde (Anhang I.C)

Die zuständige Aufsichtsbehörde bestimmt sich nach Klausel 13 der SCC wie folgt: (a) ist der Kunde in der EU niedergelassen, die Aufsichtsbehörde seiner Niederlassung; (b) ist der Kunde nicht in der EU niedergelassen, hat er aber einen Vertreter nach Art. 27 DSGVO benannt, die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter niedergelassen ist; (c) andernfalls die Aufsichtsbehörde des Mitgliedstaats, in dem sich die betroffenen Personen befinden. Für Übermittlungen nach dem UK Addendum der UK Information Commissioner; für Übermittlungen nach dem DSG der EDÖB.

Anlage 2: Technische und organisatorische Maßnahmen (Anhang II der SCC)

Der Anbieter betreibt die Services als Cloud-Anwendungen auf der Infrastruktur seiner Unterauftragsverarbeiter. Eigene Rechenzentren oder Anwendungsserver betreibt der Anbieter für die Services nicht. Die physische Sicherheit der Rechenzentren gewährleisten die Infrastruktur-Unterauftragsverarbeiter. Die folgenden Maßnahmen beschreiben, was der Anbieter umsetzt. Eigene Zertifizierungen (etwa ISO/IEC 27001 oder SOC 2) beansprucht der Anbieter nicht. Soweit verfügbar, stützt er sich auf die Zertifizierungen und Prüfberichte seiner Unterauftragsverarbeiter.

1. Vertraulichkeit

1.1 **Transportverschlüsselung:** Alle Verbindungen zu den Services nutzen TLS 1.2 oder höher.

1.2 **Verschlüsselung im Ruhezustand:** Daten in Datenbank und Speicher werden von AWS und Supabase mit AES-256 verschlüsselt.

1.3 **Mandantentrennung:** Jede Kundenorganisation ist in der Datenbank logisch durch PostgreSQL Row Level Security (RLS) getrennt. Die RLS-Richtlinien wurden in einem Security-Review 2026 verifiziert.

1.4 **Authentifizierung:** Zwei-Faktor-Authentifizierung (TOTP) ist für die Superadmins des Anbieters Pflicht und für Administratoren des Kunden verfügbar. Im HR-Modul ist Zwei-Faktor-Authentifizierung für Administratoren Pflicht.

1.5 **Berechtigungen:** Rollen- und Rechtekonzept pro Organisation; der Kunde weist seinen Authorised Users Rollen zu.

1.6 **Minimale Rechte und Secrets:** Service-Keys werden nach dem Least-Privilege-Prinzip vergeben; Secrets werden ausschließlich serverseitig gespeichert und verwendet und nicht an Client-Anwendungen ausgegeben.

1.7 **Hashing:** PINs für Zeiterfassungsterminals und API-Keys werden ausschließlich als gepfefferte Hashes gespeichert.

1.8 **Zugriff durch den Anbieter:** Der Anbieter greift auf Kunden-personenbezogene Daten nur zur Unterstützung oder auf Weisung des Kunden zu (Abschnitt 5.2 der AVV).

1.9 **Vertraulichkeit der Personen:** Alle Personen mit Zugriff sind zur Vertraulichkeit verpflichtet. Der Anbieter ist ein Ein-Personen-Betrieb; die Vertretung ist in der Vertretungsregelung des Operating Agreement des Anbieters geregelt.

1.10 **Kein KI-Training:** Kunden-personenbezogene Daten werden nicht zum Training von KI-Modellen verwendet.

2. Integrität

2.1 **Audit-Logs:** Administrative Aktionen werden protokolliert.

2.2 **Unveränderliche Zustimmungsprotokolle:** Zustimmungen zu Vertragsdokumenten (einschließlich der Terms und dieser AVV) werden in Protokollen gespeichert, die nicht verändert werden können.

2.3 **Audit-Trail der elektronischen Signatur:** Im Booking-Modul werden Signaturereignisse (Linkaufruf, OTP-Verifizierung, Zeitstempel, IP-Adresse, User-Agent) in einem Audit-Trail erfasst.

2.4 **Missbrauchsschutz:** Rate-Limiting und Bot-Schutz (Honeypot) bei der Registrierung.

2.5 **Integrität bei der Übertragung:** TLS schützt Daten bei der Übertragung vor Veränderung.

3. Verfügbarkeit

3.1 **Backups:** tägliche Backups der Datenbank durch den Datenbankanbieter (Supabase).

3.2 **Verteilte Auslieferung:** App-Auslieferung über das globale Edge-Netzwerk von Cloudflare.

3.3 **Monitoring:** Überwachung der Services mit Alarmierung.

3.4 **Offline-Modus:** Das HR-Terminal kann Arbeitszeiten offline erfassen und synchronisiert die Einträge, sobald die Verbindung wiederhergestellt ist.

4. Belastbarkeit

4.1 **Verwaltete Infrastruktur:** Nutzung verwalteter Datenbank-, Speicher- und Edge-Infrastruktur etablierter Anbieter statt selbst betriebener Server.

4.2 **Incident-Prozess:** definierter Prozess zur Erkennung, Bewertung, Eindämmung und Meldung von Sicherheitsvorfällen, gestützt auf Monitoring und Alarmierung.

4.3 **Betriebskontinuität:** Vertretung des alleinigen Betreibers nach der Vertretungsregelung im Operating Agreement des Anbieters.

5. Wiederherstellung der Verfügbarkeit und des Zugangs

5.1 Wiederherstellung aus den täglichen Backups des Datenbankanbieters.

5.2 Backups werden höchstens 90 Tage nach Löschung der Daten im Produktivsystem aufbewahrt (Abschnitt 10.2 der AVV).

6. Regelmäßige Überprüfung, Bewertung und Evaluierung

6.1 Überprüfung der Mandantentrennung (RLS-Richtlinien), zuletzt verifiziert in einem Security-Review 2026.

6.2 Auswertung von Monitoring-Alarmen und Vorfällen im Rahmen des Incident-Prozesses.

6.3 Überprüfung der Maßnahmen dieser Anlage bei wesentlichen Änderungen der Services, insbesondere vor dem Go-live neuer Module.

7. Datenminimierung, Aufbewahrung und Löschung

7.1 Löschkonzept mit festgelegtem Exportfenster und Löschfristen (Abschnitt 10 der AVV): 90 Tage Export nach Ende des Vertrags, eines Abonnements oder einer nicht umgewandelten Testphase, Löschung innerhalb weiterer 30 Tage, Backups innerhalb von 90 Tagen.

7.2 Der Kunde kann einzelne Datensätze jederzeit mit den Funktionen der Services löschen.

8. Maßnahmen in Bezug auf Unterauftragsverarbeiter

8.1 Auswahl von Unterauftragsverarbeitern, die hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bieten.

8.2 Verträge, die die Anforderungen von Art. 28 Abs. 3 und 4 DSGVO erfüllen, und geeignete Garantien für Übermittlungen nach Kapitel V DSGVO (DPF-Zertifizierung des Unterauftragsverarbeiters, soweit vorhanden, andernfalls Standardvertragsklauseln).

8.3 Wahl von EU-Hosting-Regionen für die Datenbanken (Frankfurt und Irland), soweit angeboten.

8.4 Prüfung der Unterauftragsverarbeiter vor der Beauftragung und bei wesentlichen Änderungen ihrer Dienste oder Bedingungen; Mitteilung von Änderungen nach Abschnitt 6 der AVV.

9. Maßnahmen in Bezug auf behördliche Zugriffe (Klausel 15 der SCC)

9.1 Hosting der Kunden-personenbezogenen Daten in EU-Regionen (Ziffer 8.3), Verschlüsselung bei der Übertragung und im Ruhezustand.

9.2 Prüfung jedes Ersuchens auf Rechtmäßigkeit, Anfechtung rechtswidriger Ersuchen und Offenlegung nur der erforderlichen Mindestdaten (Abschnitt 12 der AVV).

9.3 Benachrichtigung des Kunden, sofern nicht untersagt, und Bemühen nach besten Kräften um Aufhebung eines Verbots.

9.4 Dokumentation von Ersuchen, rechtlichen Beurteilungen und Anfechtungen; Transparenzinformationen an den Kunden auf Anfrage.

9.5 Keine Hintertüren (Abschnitt 12.6 der AVV).

10. Maßnahmen zur Unterstützung des Kunden

10.1 Funktionen zum Suchen, Berichtigen, Exportieren und Löschen von Daten zur Unterstützung bei Anträgen betroffener Personen (Abschnitt 7 der AVV).

10.2 Exportfunktionen für Kundendaten (Abschnitt 10.1 der AVV und Schedule 4 der Terms).

Anlage 3: Unterauftragsverarbeiter (Anhang III der SCC)

Die aktuelle Liste der Unterauftragsverarbeiter ist unter growmino.de/legal/subprocessors veröffentlicht. Änderungen erfolgen nach Abschnitt 6 der AVV. Zum Inkrafttreten (1. Dezember 2026) genehmigt der Kunde folgende Unterauftragsverarbeiter:

Unterauftragsverarbeiter	Leistung	Module	Ort / Region
Supabase Inc. (USA), auf Amazon Web Services	Datenbank, Authentifizierung, Speicher	CRM, Booking, HR	CRM: AWS eu-central-1 (Frankfurt, Deutschland); Booking: AWS eu-west-1 (Irland); HR: AWS eu-central-1 (Frankfurt, Deutschland). Support- und Admin-Zugriffe aus den USA möglich
Lovable Labs Incorporated / Lovable (Schweden)	App-Hosting über Cloudflare Workers, Build, Transaktions-E-Mails über notify.growmino.de, AI Gateway	Alle Module	EU, USA, globale Edge
Cloudflare, Inc. (USA)	CDN, Edge-Ausführung	Alle Module	Global
Google LLC (USA) / Google Ireland Limited (Irland)	KI-Modelle (Gemini) über das Lovable AI Gateway für Transkription und Texterstellung	CRM (KI-Transkription und -Zusammenfassungen), Booking (KI-Angebote und -Texte)	USA, EU
Twilio Inc. (USA)	Telefonie, SMS, Anrufaufzeichnungen und Voicemail	CRM (soweit die Telefonie des Anbieters genutzt wird)	USA

Unterauftragsverarbeiter	Leistung	Module	Ort / Region
Hostinger International Ltd. (Zypern), Server in Litauen	VPS-Hosting	Nur Professional Services (vom Anbieter für den Kunden im Rahmen eines SOW betriebene Websites); keine Kundendaten aus den Growmino-One-Anwendungen	Litauen, EU
Google Ireland Limited (Irland) / Google LLC (USA), Google Workspace	Geschäftliches E-Mail-Postfach, Kalender und Dateiablage des Anbieters für Support, Projektkommunikation und Dateiaustausch	Alle Module und Professional Services	EU, USA

Keine Unterauftragsverarbeiter: Stripe Payments Europe, Limited und Stripe, Inc. (eigenständige Verantwortliche für Zahlungen); vom Kunden verbundene Dienste einschließlich der eigenen Google-Workspace-, Microsoft-365- und Twilio-Konten des Kunden.