RECHTLICHES

Sicherheit und Informationen nach dem Data Act

Version
v2026–12–01
Gültig ab
1. Dezember 2026
SHA-256
1e2df6e2a2604383dc81ed5ec2daefa1887b0065ce5ec015df2d13e0180ebf5e

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

> Unverbindliche Übersetzung. Maßgeblich ist die englische Fassung.

Sicherheit und Informationen nach dem Data Act

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

Diese Seite erklärt verständlich, wie die PUSH - CONSULTING LLC, 30 N Gould St Ste N, Sheridan, WY 82801, USA, Wyoming Secretary of State Filing ID 2026-002106936 („wir“, „Anbieter“), die Daten in den Growmino-One-Anwendungen schützt. Sie enthält außerdem die Informationen, die wir nach Art. 26 und Art. 28 der Verordnung (EU) 2023/2854 (EU Data Act) veröffentlichen müssen, sowie unsere Kontaktstelle nach der Verordnung (EU) 2022/2065 (Digital Services Act). Die verbindlichen technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 2 unserer Auftragsverarbeitungsvereinbarung (AVV). Diese Seite dient der Information und erweitert sie nicht.

---

1. Überblick über unsere Sicherheitsmaßnahmen

1.1 **Wie wir arbeiten.** Growmino One CRM, Booking und HR laufen als Cloud-Anwendungen auf verwalteter Infrastruktur etablierter Anbieter. Eigene Rechenzentren oder Anwendungsserver betreiben wir für diese Anwendungen nicht. Die physische Sicherheit der Rechenzentren gewährleisten unsere Infrastrukturanbieter.

1.2 **Ehrlicher Umfang.** Wir beschreiben nur Maßnahmen, die tatsächlich umgesetzt sind. Eigene Zertifizierungen (etwa ISO/IEC 27001 oder SOC 2) haben wir nicht. Soweit verfügbar,

stützen wir uns auf die Zertifizierungen und Prüfberichte unserer Unterauftragsverarbeiter.

1.3 **Kurz gesagt:**

- verschlüsselte Verbindungen (TLS 1.2 oder höher) und Verschlüsselung im Ruhezustand (AES-256);
- strikte Trennung der Kundenorganisationen in der Datenbank (Row Level Security);
- Zwei-Faktor-Authentifizierung, Rollen und Berechtigungen;
- tägliche Backups durch unseren Datenbankanbieter;
- Monitoring mit Alarmierung und ein definierter Incident-Prozess;
- keine Nutzung Ihrer Daten für KI-Training.

---

2. Datenstandorte je Anwendung

Anwendung	Datenbank, Authentifizierung und Dateispeicher	Auslieferung der Anwendung
Growmino One CRM	Supabase auf AWS eu-central-1 (Frankfurt, Deutschland)	Lovable / Cloudflare globale Edge
Growmino One Booking	Supabase auf AWS eu-west-1 (Irland)	Lovable / Cloudflare globale Edge
Growmino One HR	Supabase auf AWS eu-central-1 (Frankfurt, Deutschland)	Lovable / Cloudflare globale Edge

2.1 **Edge.** Die Anwendungen werden über das globale Edge-Netzwerk von Cloudflare ausgeliefert. Anfragen werden während der Übertragung am dem Nutzer nächstgelegenen Edge-Standort verarbeitet. Die Edge ist nicht der primäre Speicherort Ihrer Daten.

2.2 **Weitere Standorte.** Anrufe, SMS und Anrufaufzeichnungen im CRM verarbeitet Twilio in den USA, soweit Sie unsere Telefonie nutzen. KI-Funktionen (Transkription, Zusammenfassungen, KI-Angebote und -Texte) werden von Google-Modellen über das Lovable AI Gateway in den USA oder der EU verarbeitet. Unsere Infrastrukturanbieter und wir selbst können für Support und Administration aus den USA aus der Ferne auf Daten zugreifen. Die vollständige Liste finden Sie unter growmino.de/legal/subprocessors.

---

3. Verschlüsselung

3.1 **Bei der Übertragung:** Alle Verbindungen zu den Anwendungen nutzen TLS 1.2 oder höher.

3.2 **Im Ruhezustand:** Daten in Datenbank und Dateispeicher werden von AWS und Supabase mit AES-256 verschlüsselt.

3.3 **Secrets und Zugangsdaten:** Secrets werden ausschließlich serverseitig gespeichert und verwendet und nie an den Browser übertragen. PINs für HR-Zeiterfassungsterminals und API-Keys werden ausschließlich als gepfefferte Hashes gespeichert.

---

4. Trennung der Kunden (Mandantenfähigkeit)

4.1 Jede Kundenorganisation ist in der Datenbank logisch durch PostgreSQL Row Level Security (RLS) getrennt. Ein Nutzer kann nur Daten der Organisation lesen und ändern, der er angehört, und nur im Rahmen der Rechte seiner Rolle.

4.2 Die RLS-Richtlinien wurden in einem Security-Review 2026 verifiziert.

---

5. Zugriffskontrolle

5.1 **Zwei-Faktor-Authentifizierung (TOTP):** Pflicht für unsere Superadmins, verfügbar für Ihre Administratoren und Pflicht für Administratoren in Growmino One HR.

5.2 **Rollen und Berechtigungen:** Jede Organisation hat ein eigenes Rollen- und Rechtekonzept. Sie entscheiden, welche Nutzer welche Rechte haben.

5.3 **Minimale Rechte:** Service-Keys erhalten nur die Rechte, die sie benötigen.

5.4 **Audit-Logs:** Administrative Aktionen werden protokolliert. Zustimmungen zu Vertragsdokumenten werden in unveränderlichen Protokollen gespeichert. In Booking werden elektronische Signaturen mit einem Audit-Trail dokumentiert.

5.5 **Unser Zugriff auf Ihre Daten:** Wir greifen auf Ihre Daten nur zu, um von Ihnen angefragten Support zu leisten oder auf Ihre Weisung, sowie soweit erforderlich, um die Anwendungen sicher und lauffähig zu halten. Growmino One wird von einer Person betrieben, die zur Vertraulichkeit verpflichtet ist; eine Vertretung wird vor Erhalt des Zugriffs zur Vertraulichkeit verpflichtet.

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

---

6. Backups und Löschung

6.1 Unser Datenbankanbieter (Supabase) erstellt tägliche Backups der Datenbank.

6.2 Nach Ende Ihres Vertrags oder Abonnements können Sie Ihre Daten 90 Tage lang exportieren (bis Tag 59 mit Lesezugriff, ab Tag 60 nur noch Export). Danach löschen wir sie innerhalb von 30 Tagen. Kopien in Backups werden innerhalb von 90 Tagen gelöscht. Dasselbe gilt, wenn eine kostenlose Testphase ohne kostenpflichtigen Plan endet.

---

7. Sicherheitsvorfälle

7.1 Wir überwachen die Anwendungen mit Alarmierung und folgen einem definierten Incident-Prozess zur Erkennung, Bewertung, Eindämmung und Meldung.

7.2 Betrifft eine Verletzung des Schutzes personenbezogener Daten Ihre Daten, benachrichtigen wir Ihre Administratoren unverzüglich und, soweit möglich, innerhalb von 48 Stunden mit den nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen, soweit bekannt, und unterstützen Sie bei Ihren eigenen Meldungen (Abschnitt 8 AVV).

---

8. Sicherheitsprobleme melden

8.1 Bitte melden Sie Sicherheitslücken, vermutete Vorfälle oder verdächtige Aktivitäten per E-Mail an **office@growmino.de** mit dem Betreff **„Security“**.

8.2 Bitte geben Sie eine Beschreibung, die betroffene Anwendung oder Adresse und nach Möglichkeit die Schritte zur Reproduktion an. Bitte greifen Sie bei Ihrer Untersuchung nicht auf Daten anderer Nutzer zu, ändern oder löschen Sie diese nicht, und geben Sie uns vor einer Veröffentlichung angemessene Zeit zur Behebung.

---

9. Rechtsordnung der Infrastruktur und Schutz vor unrechtmäßigem staatlichem Zugriff (Art. 28 EU Data Act)

9.1 **Rechtsordnung der IKT-Infrastruktur.** Die für die Datenverarbeitung der Growmino-One-Anwendungen eingesetzte Infrastruktur unterliegt folgenden Rechtsordnungen:

Beteiligter	Rolle	Rechtsordnung
PUSH - CONSULTING LLC	Anbieter der Services	USA (Bundesstaat Wyoming)

Beteiligter	Rolle	Rechtsordnung
Supabase Inc.	Datenbank, Authentifizierung, Speicher (Rechenzentren in Deutschland und Irland, betrieben von Amazon Web Services)	USA; Rechenzentren in der EU
Cloudflare, Inc.	CDN und Edge-Ausführung	USA; globales Netzwerk
Twilio Inc.	Telefonie und SMS	USA
Lovable (Schweden) / Lovable Labs Incorporated	App-Hosting, Build, Transaktions-E-Mails, AI Gateway	Schweden (EU) und USA
Google LLC / Google Ireland Limited	KI-Modelle	USA und Irland (EU)

Das Recht der USA kann daher auf uns und auf mehrere unserer Anbieter anwendbar sein, auch wenn Daten in der EU gespeichert sind.

9.2 **Maßnahmen gegen unrechtmäßigen internationalen staatlichen Zugriff oder unrechtmäßige Übermittlung.**

- **Technisch:** Speicherung der Anwendungsdatenbanken in EU-Regionen (Frankfurt und Irland); Verschlüsselung bei der Übertragung und im Ruhezustand; Mandantentrennung; Zugriffskontrolle mit Zwei-Faktor-Authentifizierung.
- **Organisatorisch:** Jedes Ersuchen einer Behörde wird auf seine Rechtmäßigkeit geprüft; rechtswidrige Ersuchen werden angefochten, einschließlich durch Beantragung einstweiliger Maßnahmen; wir legen nur die erforderlichen Mindestdaten offen; wir benachrichtigen Sie, sofern nicht gesetzlich untersagt, und bemühen uns nach besten Kräften um die Aufhebung eines Verbots; wir dokumentieren Ersuchen und unsere Beurteilung und stellen auf Anfrage Transparenzinformationen bereit. Hintertüren haben wir nicht eingebaut.
- **Vertraglich:** Die AVV enthält diese Zusagen in Abschnitt 12, entsprechend Klausel 15 der EU-Standardvertragsklauseln (SCC), die wir als Module 2 und 3 vereinbart haben, soweit Kapitel V DSGVO anwendbar ist. Unsere Unterauftragsverarbeiter sind an Datenschutzbedingungen gebunden, die der AVV gleichwertig sind, einschließlich geeigneter Übermittlungsgarantien (SCC und, soweit vorhanden, ihre Zertifizierung nach dem EU-U.S. Data Privacy Framework). Eine eigene Zertifizierung nach dem Data Privacy Framework beanspruchen wir nicht.

9.3 Für nicht-personenbezogene Daten wenden wir nach Art. 32 EU Data Act dieselben Maßnahmen zur Prüfung, Anfechtung, Minimierung und Benachrichtigung an.

10. Anbieterwechsel und Datenexport (Art. 26 EU Data Act)

10.1 **Verfahren.** Das Verfahren für den Wechsel zu einem anderen Anbieter oder in Ihre eigene Infrastruktur, einschließlich Kündigungsfrist, Übergangszeitraum, Datenabruf, Löschung und anfallender Entgelte, ist in Schedule 4 (Switching and Exit) unserer Customer Terms of Service geregelt. Sie können es in der Anwendung oder per E-Mail an office@growmino.de einleiten.

10.2 **Exportmethoden und -formate.**

Exportierbare Daten werden in strukturierten, gängigen und maschinenlesbaren Formaten bereitgestellt, insbesondere CSV und JSON; Dokumente und Rechnungen als PDF (und, soweit einschlägig, ZUGFeRD-XML); hochgeladene Dateien und Aufzeichnungen im Originalformat; sowie über die dokumentierten APIs, soweit vorhanden. Insbesondere:

- **CRM:** Leads, Kontakte, Deals, Listen, Notizen und Anrufdaten; Zugriff über API und Webhooks.
- **Booking:** Buchungen, Angebote, Verträge einschließlich Audit-Trail der elektronischen Signaturen, Rechnungen (PDF und ZUGFeRD), Dokumente und Vorlagen.
- **HR:** Zeit-, Abwesenheits- und Dienstplandaten einschließlich DATEV-Export; Zugriff über die REST-API im Enterprise-Plan.

Verbindlich legen die Ziffern 5 bis 7 von Anlage 4 (Schedule 4) die exportierbaren Daten, die vom Export ausgenommenen Daten und die Formate fest.

10.3 **Einschränkungen und technische Grenzen.** Growmino-One-spezifische Konfigurationen (etwa Workflows, Automatisierungen und Dashboard-Definitionen) werden als Daten exportiert, funktionieren im System eines anderen Anbieters aber nicht ohne Anpassung. Nicht exportierbar sind insbesondere Quellcode, interne Systemprotokolle des Anbieters und sicherheitsrelevante Daten wie Schlüssel sowie gepfefferte PIN- und API-Key-Hashes (Anlage 4 Ziffer 6). Für Daten in Ihren eigenen verbundenen Diensten (Google, Microsoft, Zapier, Ihr eigenes Twilio-Konto) gelten Ihre Verträge mit diesen Anbietern. Die Nutzung der API unterliegt den Grenzen Ihres Plans. Werden weitere Einschränkungen bekannt, die den Wechsel beeinträchtigen können, informieren wir Sie.

10.4 **Wechselentgelte.** Wir erheben keine Wechselentgelte und keine Entgelte für den Datenausgang (Egress). Die Entgelte für die während der Kündigungs- und Übergangsfristen genutzten Services bleiben geschuldet (Schedule 4).

11. Kontaktstelle nach dem Digital Services Act

11.1 Unsere zentrale Kontaktstelle für Behörden der EU-Mitgliedstaaten, die Europäische Kommission, das Europäische Gremium für digitale Dienste und für Nutzer des Dienstes (Art.

11 und 12 DSA) ist **office@growmino.de**. Die Kommunikation ist auf **Englisch und Deutsch** möglich.

11.2 Meldungen rechtswidriger Inhalte (Art. 16 DSA) können an office@growmino.de mit dem Betreff **„DSA Notice“** gesendet werden. Bitte geben Sie an, warum Sie den Inhalt für rechtswidrig halten, wo genau er zu finden ist, Ihren Namen und Ihre E-Mail-Adresse (außer bei Meldungen zu bestimmten Straftaten im Zusammenhang mit sexuellem Missbrauch von Kindern) sowie eine Erklärung, dass die Meldung nach Ihrer redlichen Überzeugung richtig und vollständig ist.

11.3 Schränken wir Inhalte oder ein Konto ein, erhalten Sie eine Begründung und Informationen über Rechtsbehelfe (Art. 17 DSA).

11.4 **Gesetzlicher Vertreter (Art. 13 DSA).** Da wir keine Niederlassung in der EU haben, haben wir als unseren gesetzlichen Vertreter in der Union benannt: David Wolff, Einzelunternehmen, Grüne Gärtel 7, 76316 Malsch, Deutschland, office@growmino.de, +49 176 31685433.

---

12. Kein Werbe-Tracking

In unseren Apps nutzen wir kein Werbe-Tracking.

---

13. Weitere Informationen

13.1 Auftragsverarbeitungsvereinbarung: Anlage 3 (Schedule 3) der Customer Terms of Service, growmino.de/legal/dpa. Unterauftragsverarbeiter: growmino.de/legal/subprocessors. Datenschutzerklärung: growmino.de/legal/privacy. Diese Seite: growmino.de/legal/security.

13.2 Kontakt: PUSH - CONSULTING LLC, 30 N Gould St Ste N, Sheridan, WY 82801, USA, office@growmino.de, +49 176 31685433. EU-Vertreter nach Art. 27 DSGVO: David Wolff, Einzelunternehmen, Grüne Gärtel 7, 76316 Malsch, Deutschland, office@growmino.de.