LEGAL

Security & Data Act Information

Version
v2026–12–01
Effective
1 December 2026
SHA-256
b2e97c84816e51017a2d0c6900657fc01840a5a49660d1b2de513dce5aac5173

The English version prevails.

Security & Data Act Information

Version v2026-12-01 · Effective 1 December 2026

This page explains in plain language how PUSH - CONSULTING LLC, 30 N Gould St Ste N, Sheridan, WY 82801, USA, Wyoming Secretary of State Filing ID 2026-002106936 ("we", "Provider"), protects the data in the Growmino One applications. It also contains the information we must publish under Art. 26 and Art. 28 of Regulation (EU) 2023/2854 (EU Data Act) and our point of contact under Regulation (EU) 2022/2065 (Digital Services Act). The binding technical and organisational measures are set out in Appendix 2 of our Data Processing Addendum (DPA). This page is for information and does not extend them.

---

1. Overview of our security measures

1.1 **How we operate.** Growmino One CRM, Booking and HR run as cloud applications on managed infrastructure of established providers. We operate no data centres or application servers of our own for these applications. Physical security of the data centres is provided by our infrastructure providers.

1.2 **Honest scope.** We describe only measures that are actually in place. We do not hold certifications of our own (such as ISO/IEC 27001 or SOC 2). Where available, we rely on the certifications and audit reports of our sub-processors.

1.3 **In brief:**

- encrypted connections (TLS 1.2 or higher) and encryption at rest (AES-256);
- strict separation of customer organisations in the database (Row Level Security);
- two-factor authentication, roles and permissions;

- daily backups by our database provider;
- monitoring with alerts and a defined incident process;
- no use of your data for AI training.

---

2. Data locations per application

Application	Database, authentication and file storage	Delivery of the application
Growmino One CRM	Supabase on AWS eu-central-1 (Frankfurt, Germany)	Lovable / Cloudflare global edge
Growmino One Booking	Supabase on AWS eu-west-1 (Ireland)	Lovable / Cloudflare global edge
Growmino One HR	Supabase on AWS eu-central-1 (Frankfurt, Germany)	Lovable / Cloudflare global edge

2.1 **Edge.** The applications are delivered through Cloudflare's global edge network. Requests are processed at the edge location closest to the user while in transit. The edge is not the primary storage location of your data.

2.2 **Other locations.** Call handling, SMS and call recordings in the CRM are processed by Twilio in the USA where you use our telephony. AI functions (transcription, summaries, AI offers and texts) are processed by Google models via the Lovable AI Gateway in the USA or the EU. Our infrastructure providers and we ourselves may access data remotely from the USA for support and administration. The full list is at growmino.de/legal/subprocessors.

---

3. Encryption

3.1 **In transit:** all connections to the applications use TLS 1.2 or higher.

3.2 **At rest:** data in the database and file storage is encrypted by AWS and Supabase using AES-256.

3.3 **Secrets and credentials:** secrets are stored and used only on the server side and are never sent to the browser. PINs for HR time-recording terminals and API keys are stored only as peppered hashes.

4. Separation of customers (multi-tenancy)

4.1 Each customer organisation is logically separated in the database through PostgreSQL Row Level Security (RLS). A user can only read and change data of the organisation to which they belong, within the permissions of their role.

4.2 The RLS policies were verified in a security review in 2026.

5. Access control

5.1 **Two-factor authentication (TOTP):** mandatory for our superadmins, available for your administrators, and mandatory for administrators in Growmino One HR.

5.2 **Roles and permissions:** every organisation has its own role and permission concept. You decide which users have which rights.

5.3 **Least privilege:** service keys are granted only with the rights they need.

5.4 **Audit logs:** administrative actions are logged. Acceptances of contract documents are stored in records that cannot be altered. In Booking, electronic signatures are documented with an audit trail.

5.5 **Our access to your data:** we access your data only to provide support you request or on your instructions, and to the extent necessary to keep the applications secure and running. Growmino One is run by one person, who is bound to confidentiality; any substitute is bound to confidentiality before gaining access.

5.6 **Abuse protection:** rate limiting and bot protection (honeypot) at registration.

6. Backups and deletion

6.1 Our database provider (Supabase) creates daily backups of the database.

6.2 After the end of your contract or subscription you can export your data for 90 days (read-only access until day 59, export only from day 60). We then delete it within 30 days. Copies in backups are deleted within 90 days. The same applies if a free trial ends without a paid plan.

7. Security incidents

7.1 We monitor the applications with alerts and follow a defined incident process for detection, assessment, containment and reporting.

7.2 If a personal data breach affects your data, we notify your administrators without undue delay and, where feasible, within 48 hours, with the information required under Art. 33(3) GDPR as far as it is known, and we support you with your own notifications (Section 8 DPA).

8. Reporting a security issue

8.1 Please report security vulnerabilities, suspected incidents or suspicious activity by e-mail to **office@growmino.de** with the subject line **"Security"**.

8.2 Please include a description, the affected application or address, and, where possible, steps to reproduce. Please do not access, change or delete data of other users while investigating, and give us reasonable time to remedy the issue before any disclosure.

9. Infrastructure jurisdiction and protection against unlawful governmental access (Art. 28 EU Data Act)

9.1 **Jurisdiction of the ICT infrastructure.** The infrastructure deployed for data processing of the Growmino One applications is subject to the following jurisdictions:

Party	Role	Jurisdiction
PUSH - CONSULTING LLC	Provider of the Services	USA (State of Wyoming)
Supabase Inc.	Database, authentication, storage (data centres in Germany and Ireland operated by Amazon Web Services)	USA; data centres in the EU
Cloudflare, Inc.	CDN and edge execution	USA; global network
Twilio Inc.	Telephony and SMS	USA
Lovable (Sweden) / Lovable Labs Incorporated	Application hosting, build, transactional e-mail, AI Gateway	Sweden (EU) and USA

Party	Role	Jurisdiction
Google LLC / Google Ireland Limited	AI models	USA and Ireland (EU)

As a result, the laws of the USA can apply to us and to several of our providers even where data is stored in the EU.

9.2 **Measures against unlawful international governmental access or transfer.**

- **Technical:** storage of the application databases in EU regions (Frankfurt and Ireland); encryption in transit and at rest; tenant separation; access control with two-factor authentication.
- **Organisational:** every request from a public authority is reviewed for lawfulness; unlawful requests are challenged, including by seeking interim measures; we disclose only the minimum data required; we notify you unless legally prohibited and use our best efforts to have any prohibition lifted; we document requests and our assessment and provide transparency information on request. We have not built any back doors.
- **Contractual:** the DPA contains these commitments in Section 12, corresponding to Clause 15 of the EU Standard Contractual Clauses (SCC), which we have agreed as Modules 2 and 3 to the extent Chapter V GDPR applies. Our sub-processors are bound by data protection terms equivalent to the DPA, including appropriate transfer safeguards (SCC and, where available, their certification under the EU-U.S. Data Privacy Framework). We do not claim a Data Privacy Framework certification of our own.

9.3 Regarding non-personal data, we apply the same review, challenge, minimisation and notification measures in accordance with Art. 32 EU Data Act.

---

10. Switching and data export (Art. 26 EU Data Act)

10.1 **Procedure.** The procedure for switching to another provider or to your own infrastructure, including notice, the transitional period, data retrieval, erasure and the applicable fees, is set out in Schedule 4 (Switching and Exit) of our Customer Terms of Service. You can initiate it in the application or by e-mail to office@growmino.de.

10.2 **Export methods and formats.**

Exportable data is made available in structured, commonly used and machine-readable formats, in particular CSV and JSON; documents and invoices as PDF (and ZUGFeRD XML where applicable); uploaded files and recordings in their original format; and via the documented APIs where available. In particular:

- **CRM:** leads, contacts, deals, lists, notes and call data; access via API and webhooks.

- **Booking:** bookings, offers, contracts including the audit trail of electronic signatures, invoices (PDF and ZUGFeRD), documents and templates.
- **HR:** time, absence and shift data, including the DATEV export; access via the REST API in the Enterprise plan.

Paragraphs 5 to 7 of Schedule 4 define the exportable data, the data excluded from export and the formats with binding effect.

10.3 **Restrictions and technical limitations.** Configurations specific to Growmino One (for example workflows, automations and dashboard definitions) are exported as data, but cannot work as a function in another provider's system without adaptation. Not exportable are, in particular, source code, Provider's internal system logs and security-relevant data such as keys and peppered PIN and API-key hashes (Schedule 4, paragraph 6). Data in your own connected services (Google, Microsoft, Zapier, your own Twilio account) is governed by your contracts with those providers. Usage of the API is subject to the limits of your plan. We will inform you if other limitations become known that may affect switching.

10.4 **Switching charges.** We do not charge switching charges or data egress charges. Fees for the Services used during the notice and transitional periods remain payable (Schedule 4).

---

11. Point of contact under the Digital Services Act

11.1 Our single point of contact for authorities of the EU Member States, the European Commission, the European Board for Digital Services and for recipients of the service (Art. 11 and 12 DSA) is **office@growmino.de**. Communication is possible in **English and German**.

11.2 Notices of illegal content (Art. 16 DSA) can be sent to office@growmino.de with the subject line **"DSA Notice"**. Please state why you consider the content illegal, where exactly it can be found, your name and e-mail address (except for notices concerning certain offences relating to the sexual abuse of children) and a statement that the notice is accurate and complete in good faith.

11.3 If we restrict content or an account, we provide a statement of reasons and information on redress (Art. 17 DSA).

11.4 **Legal representative (Art. 13 DSA).** As we have no establishment in the EU, we have designated as our legal representative in the Union: David Wolff, sole proprietorship, Grüne Gärtel 7, 76316 Malsch, Germany, office@growmino.de, +49 176 31685433.

---

12. No advertising tracking

In our apps we do not use advertising tracking.

13. Further information

13.1 Data Processing Addendum: Schedule 3 of the Customer Terms of Service, growmino.de/legal/dpa. Sub-processors: growmino.de/legal/subprocessors. Privacy Notice: growmino.de/legal/privacy. This page: growmino.de/legal/security.

13.2 Contact: PUSH - CONSULTING LLC, 30 N Gould St Ste N, Sheridan, WY 82801, USA, office@growmino.de, +49 176 31685433. EU representative under Art. 27 GDPR: David Wolff, sole proprietor, Grüne Gärtel 7, 76316 Malsch, Germany, office@growmino.de.