LEGAL

Data Processing Addendum

Version
v2026–12–01
Effective
1 December 2026
SHA-256
670ff73f0d8b88faf0f8a40a0117b83ef08ab469bc06b71c745d7817f3c8c42d

The English version prevails.

Data Processing Addendum (Schedule 3 to the Customer Terms of Service)

Version v2026-12-01 · Effective 1 December 2026

This Data Processing Addendum ("DPA") forms part of the Customer Terms of Service of PUSH - CONSULTING LLC (the "Terms") and of every Order Form and Statement of Work ("SOW") concluded under them (together, the "Agreement"). The Customer accepts this DPA together with the Terms. No separate signature is required. This DPA applies from the first time Personal Data is uploaded to, entered into or otherwise processed through the Services, including during a Trial.

The parties are:

- the customer identified in its Growmino One account, Order Form or SOW ("Customer"); and
- PUSH - CONSULTING LLC, a limited liability company organised under the laws of the State of Wyoming, USA, 30 N Gould St Ste N, Sheridan, WY 82801, USA, Wyoming Secretary of State Filing ID 2026-002106936, represented by its Sole Member and Manager David Wolff, office@growmino.de, operating under the brands "Growmino" and "Growmino One" ("Provider").

This DPA contains all provisions required by Art. 28(3) GDPR. It applies in full on its own, irrespective of whether the Standard Contractual Clauses (Section 11) apply to a given processing operation.

1. Definitions

1.1 Capitalised terms not defined in this DPA have the meaning given in the Terms. The terms "controller", "processor", "data subject", "personal data", "processing", "supervisory authority" and "personal data breach" have the meanings given in the GDPR, and their equivalents under other Data Protection Laws are interpreted accordingly.

1.2 In this DPA:

- **"Customer Personal Data"** means Personal Data contained in Customer Data that Provider processes on behalf of Customer under the Agreement.
- **"Customer-Connected Services"** means third-party services that Customer or its Authorised Users connect to the Services under their own contract with the respective third party, in particular Customer's own Google Workspace or Google accounts, Microsoft 365 or Outlook accounts, Customer's own Twilio accounts, Customer's own advertising accounts (such as Google Ads or Meta) and Customer's own integration tools (such as Zapier).
- **"Data Protection Laws"** means all data protection laws applicable to the processing of Customer Personal Data under the Agreement, including the GDPR, the laws of the EU Member States implementing or supplementing it, the UK GDPR and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection of 25 September 2020 ("FADP"), and US State Privacy Laws.
- **"DPF"** means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework, as applicable, together with the adequacy decisions or recognitions adopted for them.
- **"GDPR"** means Regulation (EU) 2016/679.
- **"Personal Data"** means any information relating to an identified or identifiable natural person, and any information defined as "personal data", "personal information" or an equivalent term under Data Protection Laws.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed by Provider or its Sub-processors.
- **"Restricted Transfer"** means a transfer of Customer Personal Data to a third country or international organisation that is subject to Chapter V GDPR, to the equivalent rules of the UK GDPR, or to Art. 16 and 17 FADP.
- **"SCC"** means the standard contractual clauses for the transfer of personal data to third countries set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **"Sub-processor"** means any processor engaged by Provider that processes Customer Personal Data on behalf of Provider in connection with the Services.
- **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner

under section 119A of the UK Data Protection Act 2018, in force from 21 March 2022, as amended from time to time.

- **"US State Privacy Laws"** means the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA") and comparable US state privacy laws, to the extent applicable.

---

2. Scope and Roles of the Parties

2.1 **Customer as controller.** Where Customer determines the purposes and means of the processing of Customer Personal Data, Customer is the controller and Provider is Customer's processor.

2.2 **Customer as processor.** Where Customer processes Customer Personal Data on behalf of a third-party controller (for example, an agency running the Services for its own clients), Customer is a processor and Provider is a Sub-processor of Customer. Customer warrants that its controller has authorised Customer's instructions under this DPA, including the engagement of Provider and of the Sub-processors listed in Appendix 3. Customer is the single point of contact for Provider. Provider is not obliged to communicate with Customer's controller directly, except where Data Protection Laws or the SCC require it.

2.3 **Provider as independent controller.** Provider processes the following Personal Data as an independent controller and not under this DPA, in accordance with its Privacy Notice (growmino.de/legal/privacy): (a) account and registration data of Customer and its Authorised Users (such as name, business e-mail address, company, role and login credentials); (b) billing, payment, tax and contract administration data, including the immutable records of contract acceptances; (c) data processed for the security, integrity and abuse prevention of the Services (such as authentication logs, rate-limiting data and audit logs of administrative actions), to the extent these are processed for Provider's own purposes; and (d) communications between Customer and Provider (such as support requests and legal notices).

2.4 **Stripe.** Payment processing is performed by Stripe Payments Europe, Limited and Stripe, Inc. ("Stripe") as independent controllers under their own terms and privacy policies. Stripe is not a Sub-processor of Provider.

2.5 **Customer-Connected Services.** Customer-Connected Services are services of Customer. Their providers are not Sub-processors of Provider. Customer is responsible for its contracts with those providers, for the lawfulness of the data flows it initiates between the Services and Customer-Connected Services, and for the settings within them. Provider processes data received from or sent to Customer-Connected Services as Customer's processor under this DPA.

2.6 **Customer's responsibilities.** Customer is solely responsible for (a) the lawfulness of the processing of Customer Personal Data, including the existence of a legal basis; (b) informing data subjects in accordance with Art. 13 and 14 GDPR; (c) obtaining any consent required by

law, in particular for the recording of telephone calls, for the sending of marketing communications by e-mail, SMS or telephone, and for the processing of data of minors; (d) complying with employment law and co-determination requirements when using the HR module, including any consultation of a works council; (e) the accuracy and quality of Customer Personal Data; and (f) entering special categories of Personal Data within the meaning of Art. 9 GDPR or data relating to criminal convictions and offences within the meaning of Art. 10 GDPR only where Data Protection Laws permit it and, where the Services provide designated fields for such data, only in those fields.

2.7 **No AI training.** Provider does not use Customer Personal Data to train artificial intelligence models and does not permit its Sub-processors to do so.

---

3. Details of Processing

3.1 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of data subjects are set out in Appendix 1, separately for each Module and for Professional Services.

3.2 The duration of the processing corresponds to the term of the Agreement plus the periods for export and deletion set out in Section 10.

---

4. Instructions

4.1 **Documented instructions.** Provider processes Customer Personal Data only on documented instructions from Customer, including with regard to transfers of Customer Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law or other law to which Provider is subject. In such a case, Provider informs Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 **What counts as an instruction.** Customer's documented instructions as of the effective date of this DPA are this DPA and the Agreement. Further instructions are given (a) through the configuration and use of the Services by Customer and its Authorised Users, including settings, workflows, automations, integrations, imports, exports and deletions; and (b) in text form by e-mail to office@growmino.de. Instructions that go beyond the functionality and scope of the Agreement require a separate agreement, for which Provider may charge reasonable fees.

4.3 **Unlawful instructions.** Provider informs Customer without undue delay if, in its opinion, an instruction infringes the GDPR or other Data Protection Laws. Provider may suspend the execution of the instruction concerned until Customer confirms or changes it. Provider is not obliged to perform a comprehensive legal review of Customer's instructions.

4.4 **Purpose limitation.** Provider does not process Customer Personal Data for any purpose other than providing, maintaining, securing and supporting the Services in accordance with the Agreement and Customer's instructions.

---

5. Confidentiality and Security

5.1 **Confidentiality of personnel.** Provider ensures that all persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Provider is operated by one person. Any substitute acting under the representation arrangement in Provider's operating agreement is bound to confidentiality before gaining access. The confidentiality obligation continues after the end of the engagement.

5.2 **Access by Provider.** Provider accesses Customer Personal Data only to the extent necessary to provide support requested by Customer, to perform Customer's instructions, to maintain the security and operation of the Services, or to comply with law.

5.3 **Security measures.** Provider implements and maintains the technical and organisational measures set out in Appendix 2 to ensure a level of security appropriate to the risk within the meaning of Art. 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

5.4 **Changes.** The measures are subject to technical progress and further development. Provider may replace them with adequate alternative measures. Provider will not lower the overall level of protection during the term of the Agreement.

5.5 **Customer's own measures.** Customer is responsible for the security measures within its control, in particular for user management, the assignment of roles, the activation of two-factor authentication for its administrators where available, the protection of its credentials and API keys, and the security of its Customer-Connected Services and devices, including time-recording terminals.

---

6. Sub-processors

6.1 **General authorisation.** Customer grants general authorisation to engage the Sub-processors listed at growmino.de/legal/subprocessors. The list as of the effective date of this DPA is set out in Appendix 3.

6.2 **Notice of changes.** Provider will give at least 30 days' notice of any intended addition or replacement of a Sub-processor by e-mail and on that page. Customer administrators

receive these notices automatically. Other persons may subscribe by request to office@growmino.de.

6.3 **Objection.** Customer may object on reasonable data-protection grounds within 30 days of notice. Provider will try to propose a reasonable alternative. If none is available, Customer may terminate the affected Services effective on the date the change takes effect, with a pro-rata refund under Section 10.3(c) of the Terms. As Customer has granted general authorisation under Section 6.1, no further consent is required; if Customer does not object within the notice period, that general authorisation extends to the new Sub-processor.

6.4 **Emergency replacement.** Where an immediate replacement is necessary to maintain the security or availability of the Services, Provider may replace a Sub-processor without prior notice and will notify Customer without undue delay; Section 6.3 applies accordingly.

6.5 **Flow-down and liability.** Provider imposes on each Sub-processor, by contract or other legal act under Union or Member State law, data protection obligations equivalent to those in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the GDPR, including appropriate safeguards for transfers under Chapter V GDPR. Provider remains fully liable to Customer for the performance of its Sub-processors' obligations. Where a Sub-processor offers only standard terms, the parties agree that those terms satisfy this Section 6.5 if they meet the requirements of Art. 28(3) and (4) GDPR.

6.6 **Copies.** On request, Provider will provide Customer with information on the data protection terms agreed with a Sub-processor. Provider may remove or redact commercial information and confidential terms.

---

7. Assistance

7.1 **Data subject requests.** Taking into account the nature of the processing, Provider assists Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR. The Services provide functions to search, view, correct, export and delete Customer Personal Data. Where Customer cannot fulfil a request using these functions, Provider will provide reasonable further assistance on request.

7.2 **Requests received by Provider.** If a data subject submits a request directly to Provider that relates to Customer Personal Data, Provider will forward it to Customer without undue delay where Provider can identify Customer, and will not respond to the request itself unless authorised by Customer or required by law.

7.3 **Security, breach, DPIA and prior consultation.** Taking into account the nature of the processing and the information available to Provider, Provider assists Customer in ensuring compliance with the obligations under Art. 32 to 36 GDPR, in particular by providing information on the Services and on the measures in Appendix 2 for Customer's data

protection impact assessments and, where required, for prior consultations with the supervisory authority.

7.4 **Authorities.** Provider cooperates, on request, with the competent supervisory authority in the performance of its tasks and informs Customer without undue delay of any inspection or measure by a supervisory authority relating to Customer Personal Data, to the extent legally permitted.

7.5 **Records.** Provider maintains a record of all categories of processing activities carried out on behalf of Customer in accordance with Art. 30(2) GDPR, to the extent this obligation applies to it.

7.6 **Costs.** Assistance under this Section 7 is free of charge where it is provided through the functions of the Services or concerns a Personal Data Breach in Provider's area of responsibility. For other assistance that requires substantial effort, Provider may charge reasonable fees at its then-current rates after informing Customer in advance.

---

8. Personal Data Breach

8.1 Provider will notify Customer without undue delay, and where feasible within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Data. The notification will include, to the extent known, the information required by Art. 33(3) GDPR; Provider will provide further information in phases as it becomes available.

8.2 Provider will take reasonable measures to contain and remediate the breach and will assist Customer with its notification obligations under Art. 33 and 34 GDPR.

8.3 Provider sends notifications to the e-mail addresses of Customer's administrators stored in the account and, where Customer has designated one, to its data protection contact. Customer is responsible for keeping these addresses up to date.

8.4 Provider documents Personal Data Breaches, including the facts, effects and remedial action taken.

8.5 Provider's notification is not an acknowledgement of fault or liability.

---

9. Information and Audits

9.1 **Information.** Provider makes available to Customer all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and this DPA. Provider fulfils this obligation primarily by providing documents, including this DPA and its Appendices, the Security & Data Act Information published at growmino.de/legal/security,

written answers to reasonable security questionnaires and, where available and permitted to be shared, certifications or audit reports of its Sub-processors.

9.2 **Audits.** If the documents provided under Section 9.1 are not sufficient to demonstrate compliance, Customer may, at its own cost, carry out an audit or have it carried out by an independent auditor bound to confidentiality, not more than once in any 12-month period and with at least 30 days' prior notice in text form. Audits are carried out remotely or, where necessary, at Provider's business premises during normal business hours (CET), without undue disruption of Provider's operations and without access to the data of other customers or to Provider's confidential information unrelated to the processing of Customer Personal Data. Provider may object to an auditor who is a competitor of Provider.

9.3 **Additional audits.** Notwithstanding the frequency limit in Section 9.2, Customer may carry out an additional audit (a) following a Personal Data Breach affecting Customer Personal Data, or (b) where a competent supervisory authority requests or orders it.

9.4 **Sub-processors' facilities.** Provider operates no data centres of its own for the Services. Audits of data-centre and infrastructure measures are fulfilled through the certifications, reports and audit mechanisms that Sub-processors make available.

9.5 **SCC.** Clause 8.9 of the SCC remains unaffected. Sections 9.1 to 9.4 describe how Provider implements it.

---

10. Return and Deletion

10.1 **Export.** During the term of the Agreement Customer can export Customer Data at any time using the export functions of the Services. After termination or expiry of the Agreement, or after a Trial ends without selection of a paid Plan, Customer may export Customer Data for 90 days in accordance with the access stages in Section 10.9 of the Terms. The switching and exit rules in Schedule 4 of the Terms remain unaffected and prevail where they provide for longer periods.

10.2 **Deletion.** After the export period has expired, Provider deletes Customer Personal Data within 30 days, unless Union or Member State law or other law to which Provider is subject requires storage of the Personal Data. Copies in backups are deleted within 90 days in the ordinary backup cycle. Until their deletion, backups are kept under the measures of Appendix 2 and are not used for any other purpose.

10.3 **Earlier deletion.** Customer may delete Customer Personal Data at any time using the functions of the Services, or instruct Provider by e-mail to delete it earlier. Section 10.2 applies to backups.

10.4 **Statutory retention.** Where Provider must retain Customer Personal Data by law, Provider restricts its processing to the purposes of such retention and deletes it when the retention period ends.

10.5 **Confirmation.** On request, Provider will confirm the deletion to Customer in text form.

---

11. International Transfers and Standard Contractual Clauses

11.1 **Provider's location.** Provider is established in the USA. Customer Personal Data is hosted in the regions stated in Appendix 1 and Appendix 3. Remote access by Provider and certain Sub-processors from third countries is possible.

11.2 **Incorporation of the SCC.** To the extent the processing involves a transfer of Personal Data to a third country subject to Chapter V GDPR, and no other transfer mechanism (in particular an adequacy decision, including the EU-U.S. Data Privacy Framework) applies, the SCC are incorporated into this DPA by reference: Module 2 (controller to processor) where Customer is controller, and Module 3 (processor to processor) where Customer is processor. Customer is the data exporter and Provider is the data importer. Unless and until Provider is certified under the DPF and has notified Customer of this, transfers from Customer to Provider are based on the SCC.

11.3 **Options.** The following options apply to the SCC:

- Clause 7 (docking clause) applies.
- Clause 9(a): Option 2 (general written authorisation) applies with a notice period of 30 days. Section 6 of this DPA applies to the procedure.
- Clause 11(a): the optional wording does not apply.
- Clause 13: (a) where Customer is established in the EU, the supervisory authority of its establishment; (b) where Customer is not established in the EU but has appointed a representative under Art. 27 GDPR, the supervisory authority of the Member State in which the representative is established; (c) otherwise, the supervisory authority of the Member State in which the data subjects whose Personal Data is transferred are located.
- Clause 17: Option 1 applies; the SCC are governed by the law of Germany.
- Clause 18(b): disputes are resolved by the courts of Germany.

11.4 **Annexes.** Annex I.A: the data exporter is Customer as identified in its account, Order Form or SOW, with the contact details stored there; its activities are the use of the Services under the Agreement; the data importer is Provider with the details stated at the beginning of this DPA, acting as processor (Module 2) or sub-processor (Module 3); the parties' acceptance of the Terms constitutes signature of Annex I.A. Annex I.B: Appendix 1, per Module. Annex I.C: the competent supervisory authority determined under Clause 13 as set out in Section 11.3. Annex II: Appendix 2. Annex III: Appendix 3 and the list at growmino.de/legal/subprocessors.

11.5 **Transfer impact assessment.** Provider has assessed the laws and practices of the USA applicable to it and to its Sub-processors in accordance with Clause 14 of the SCC and will provide Customer, on request, with the information reasonably required for Customer's own assessment. Provider will notify Customer without undue delay if it has reason to believe that

it is or has become subject to laws or practices not in line with the requirements of Clause 14(a) of the SCC.

11.6 **Onward transfers.** Provider transfers Customer Personal Data onward to Sub-processors in third countries, in particular to Sub-processors established in the USA, only on the basis of (a) the DPF certification of the respective Sub-processor, where it is available and covers the processing, or (b) standard contractual clauses (Module 3, processor to processor) concluded with the Sub-processor, or (c) another appropriate safeguard under Art. 46 GDPR. This implements Clause 8.7 and Clause 9 of the SCC. Provider relies on the SCC and, where available, the Sub-processors' DPF certification. Provider does not claim a DPF certification of its own.

11.7 **United Kingdom.** For Restricted Transfers subject to the UK GDPR, the UK Addendum is incorporated by reference and applies as follows: Table 1 is completed with the information in Section 11.4 (Annex I.A); Table 2 is completed with the Modules and options selected in Section 11.3; Table 3 is completed with Appendix 1, Appendix 2 and Appendix 3; in Table 4, neither party may end the UK Addendum under its Section 19. Where the UK Extension to the DPF applies to a Sub-processor, it may be relied upon for onward transfers.

11.8 **Switzerland.** For Restricted Transfers subject to the FADP, the SCC apply with the following adaptations: references to the GDPR are read as references to the FADP; the competent supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC); data subjects in Switzerland may bring claims in Switzerland; and the term "Member State" includes Switzerland, so that data subjects with habitual residence in Switzerland are not excluded from bringing claims at their place of habitual residence.

11.9 **Other jurisdictions.** Where other Data Protection Laws require a specific transfer mechanism, the parties will cooperate in good faith to put it in place. Until then, the SCC apply accordingly to the extent permitted.

11.10 **Recital 7 note.** Where Provider is itself subject to the GDPR under Art. 3(2) GDPR for a specific processing operation, the SCC apply only to the extent this is required under Chapter V GDPR.

11.11 **Precedence of the SCC.** In case of conflict between the SCC and this DPA or the Terms, the SCC prevail. Nothing in the Agreement is intended to contradict, directly or indirectly, the SCC or to prejudice the fundamental rights or freedoms of data subjects.

---

12. Government Access Requests

12.1 **Notification.** Provider will notify Customer, and where possible the data subject, without undue delay if it (a) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination or any other third country for the disclosure of Customer Personal Data; or (b) becomes aware of any direct access by public authorities to Customer Personal Data. The notification will include information about

the Personal Data requested, the requesting authority, the legal basis for the request and the response provided.

12.2 **Prohibition of notification.** If Provider is prohibited from notifying Customer, it will use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. Provider will document its best efforts so that it can demonstrate them on request.

12.3 **Review and challenge.** Provider will review the legality of any request for disclosure, in particular whether it remains within the powers granted to the requesting authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. Provider will pursue possibilities of appeal under the same conditions. When challenging a request, Provider will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. Provider will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

12.4 **Minimisation.** Provider will provide the minimum amount of information permissible when responding to a request, based on a reasonable interpretation of the request.

12.5 **Transparency.** Provider will provide Customer, at regular intervals and on request, with as much relevant information as possible on the requests received, in particular the number of requests, the type of data requested, the requesting authorities, whether requests have been challenged and the outcome of such challenges, to the extent legally permitted. Provider will preserve the documentation of its legal assessment and of any challenge for the duration of the Agreement and make it available to the competent supervisory authority on request.

12.6 **No back doors.** Provider has not purposefully created back doors or similar programming that could be used to access the Services or Customer Personal Data, and is not required by law or practice to create or maintain them.

12.7 This Section 12 corresponds to Clause 15 of the SCC and applies irrespective of whether the SCC apply. Where the SCC apply, Clause 15 of the SCC prevails.

---

13. EU Representative

13.1 Provider has designated the following representative in the Union in accordance with Art. 27 GDPR: David Wolff, sole proprietor (Einzelunternehmen), Grüne Gärtel 7, 76316 Malsch, Germany, office@growmino.de.

13.2 The representative may be addressed, in addition to or instead of Provider, by supervisory authorities and data subjects on all issues related to processing. The representative is mandated to maintain the record of processing activities.

13.3 Provider has not designated a data protection officer, because it is not required to do so under Art. 37 GDPR.

---

14. Liability

14.1 Each party's liability under or in connection with this DPA is subject to the limitations and exclusions of liability in Section 15 of the Terms, including the Data Cap, to the extent permitted by applicable law.

14.2 Nothing in this DPA or in the Terms limits or excludes (a) the liability of either party towards data subjects, including under Art. 82 GDPR and Clause 12(b) and (c) of the SCC; (b) liability towards a supervisory authority for fines imposed on that party; or (c) any liability that cannot be limited under applicable mandatory law. The internal allocation of liability between the parties under Art. 82(5) GDPR remains unaffected.

---

15. US State Privacy Laws

To the extent the CCPA or other US State Privacy Laws apply, Provider acts as Customer's "service provider" or "processor" and (a) does not sell or share Customer Personal Data, as those terms are defined in the CCPA; (b) does not retain, use or disclose Customer Personal Data for any purpose, including any commercial purpose, other than the business purposes specified in the Agreement, or outside the direct business relationship with Customer; (c) does not combine Customer Personal Data with Personal Data received from other sources, except as permitted under the CCPA; (d) complies with the CCPA and provides the same level of privacy protection as required of businesses under it; (e) notifies Customer if it determines that it can no longer meet these obligations; and (f) permits Customer to take reasonable and appropriate steps to stop and remediate unauthorised use of Customer Personal Data. Provider certifies that it understands and will comply with these restrictions.

---

16. Term

16.1 This DPA enters into force with the acceptance of the Terms and remains in force for as long as Provider processes Customer Personal Data, irrespective of the termination of the Agreement.

16.2 Provisions that by their nature are intended to continue after the end of the processing, in particular Sections 5.1, 10, 12 and 14, survive termination.

17. Precedence and General Provisions

17.1 **Precedence.** For the processing of Personal Data, the following order of precedence applies: (1) the SCC and their Annexes, to the extent they apply; (2) this DPA; (3) the Terms and other parts of the Agreement. An Order Form or SOW prevails over this DPA only where it expressly states that it deviates from it and the deviation is permitted under Data Protection Laws.

17.2 **Governing law and disputes.** Except where the SCC apply (Section 11.3 and Clauses 17 and 18 of the SCC) and except where Data Protection Laws mandatorily require otherwise, this DPA is governed by the law and dispute resolution provisions of the Terms.

17.3 **Amendments.** Provider may amend this DPA in accordance with the procedure for amendments to the Terms. Silence or continued use does not constitute acceptance of material or detrimental amendments. Provider may update Appendix 3 in accordance with Section 6. Amendments required by a change of Data Protection Laws or by a decision of a competent authority or court may be implemented with the notice period stated in the Terms.

17.4 **Severability.** If any provision of this DPA is invalid or unenforceable, the remaining provisions remain in force. The invalid provision is replaced by a valid provision that comes as close as possible to the intended purpose, and in any case by the requirements of Art. 28(3) GDPR.

17.5 **Language.** This DPA is concluded in English. Translations are provided for convenience only. In case of conflict the English version prevails, except where mandatory law requires otherwise.

Appendix 1: Details of Processing (Annex I to the SCC)

A. List of parties (Annex I.A)

Data exporter: Customer, with the name, address and contact details stated in its account, Order Form or SOW. Activities relevant to the data transferred: use of the Growmino One Services and, where agreed, Professional Services under the Agreement. Role: controller (Module 2) or processor (Module 3). Signature and date: acceptance of the Terms in the application or signature of the Order Form or SOW.

Data importer: PUSH - CONSULTING LLC, 30 N Gould St Ste N, Sheridan, WY 82801, USA, Wyoming Secretary of State Filing ID 2026-002106936. Contact: David Wolff, Sole Member and Manager, 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. Activities relevant to the data transferred: provision, hosting, operation, support and security of the Services and performance of Professional Services. Role: processor (Module 2) or sub-processor (Module 3). Signature and date: acceptance of the Terms by Customer, which Provider confirms by providing the Services.

B. Description of transfer and processing (Annex I.B)

The following applies to all Modules unless stated otherwise:

- **Nature of processing:** collection via the Services and interfaces, storage, organisation, structuring, retrieval, consultation, use, alignment and combination as configured by Customer, transmission to recipients chosen by Customer, restriction, export and erasure.
- **Frequency of transfer:** continuous, for the duration of the Agreement.
- **Retention:** as determined by Customer through its use of the Services; at the latest until deletion under Section 10 of the DPA (90 days' export window after the end of the Agreement or Subscription, deletion within a further 30 days, backups within 90 days).
- **Users of all Modules:** Customer's Authorised Users (employees, contractors and other persons authorised by Customer). Their profile data, roles, permissions, activity and audit records within Customer's organisation are processed on behalf of Customer, without prejudice to Section 2.3 of the DPA.
- **Hosting and Sub-processor transfers:** see each Module and Appendix 3. All Modules are delivered through Lovable (application hosting, build, transactional e-mail via notify.growmino.de, AI Gateway) and Cloudflare (CDN and edge execution worldwide). Edge processing transmits data in transit and does not serve as the primary storage location.

B.1 Growmino One CRM

- **Subject matter and purpose:** management of Customer's leads, contacts, companies, deals and sales pipeline; e-mail communication and automation; calendar synchronisation; telephony and SMS; AI transcription and summary of calls; dashboards and KPIs; lists; API, webhooks, import and export.
- **Categories of data subjects:** Customer's leads, prospects, customers and their contact persons; business partners; persons who contact Customer by telephone, SMS, e-mail or web form; recipients of Customer's communications; Authorised Users.
- **Categories of Personal Data:** identity and contact data (name, title, company, position, e-mail address, telephone number, postal address); pipeline and deal data (status, value, products, stage, owner); notes, tasks, attachments and custom fields; source and campaign data received via webhooks or import (for example, lead form answers); e-mail content and metadata sent or received through Customer-Connected Services; calendar entries; call metadata (numbers, time, duration, direction, outcome); voice data, namely call recordings and voicemails; transcripts and AI-generated summaries of calls; SMS content and metadata; communication history and consent status as recorded by Customer.

- **Special categories:** not intended. If data subjects disclose special categories of Personal Data in calls, messages or notes, they are processed only as part of the respective content. Voice recordings are not processed for the purpose of uniquely identifying a natural person.
- **Processing location:** database, authentication and storage at Supabase on AWS eu-central-1 (Frankfurt, Germany).
- **Sub-processor transfers:** Supabase (hosting); Lovable and Cloudflare (application delivery, e-mail); Twilio (telephony, SMS, recordings, USA), where Customer uses Provider's telephony; Google via the Lovable AI Gateway (transcription and summaries), where Customer uses AI functions.

B.2 Growmino One Booking

- **Subject matter and purpose:** creation and management of Customer's offers, bookings and contracts with its end customers; electronic signature with audit trail via link and one-time password (OTP); invoicing by Customer to its end customers (PDF, ZUGFeRD); AI-assisted creation of offers and texts; document library.
- **Categories of data subjects:** Customer's end customers and their contact persons; participants named in bookings; signatories; Authorised Users.
- **Categories of Personal Data:** identity and contact data (name, company, postal address, e-mail address, telephone number); booking and contract data (services, dates, prices, participants, contract content, attachments and uploaded documents); signature data (name of the signatory, signature image or typed signature, e-mail address used for the signing link, OTP verification events, IP address, user agent, timestamps and audit trail entries); invoice data (invoice items, amounts, payment status, tax information provided by Customer); communication data related to bookings.
- **Special categories:** not intended. Customer may only include special categories of Personal Data in contracts or documents where Data Protection Laws permit it.
- **Processing location:** database, authentication and storage at Supabase on AWS eu-west-1 (Ireland).
- **Sub-processor transfers:** Supabase (hosting); Lovable and Cloudflare (application delivery, e-mail including signing links and OTP); Google via the Lovable AI Gateway, where Customer uses AI credits.

B.3 Growmino One HR

- **Subject matter and purpose:** time recording (including terminal with PIN and offline mode), absence management, shift planning, working time accounts, storage of payroll documents, DATEV export, location management and REST API (Enterprise).
- **Categories of data subjects:** Customer's employees, trainees, temporary workers and freelancers; Customer's managers and HR administrators; Authorised Users.
- **Categories of Personal Data:** identity and employment data (name, personnel number, location, department, role, contract type, working time model); contact data; working time data (clock-in and clock-out times, breaks, terminal and device identifiers, location assignment, offline records, corrections and approvals); working time accounts and shift

plans; absence data (type, period, status and, where entered by Customer, the reason for absence); payroll documents uploaded by Customer (which may contain salary data, tax and social security identifiers and bank details); DATEV export data; hashed terminal PINs and API key hashes; audit records.

- **Special categories:** absence reasons may disclose health data (for example sick leave), and payroll documents may contain data revealing religious affiliation (for example church tax information). Safeguards: Customer records only the information necessary for the respective purpose (for sick leave in principle only the fact and duration, not a diagnosis); access is restricted by the role and permission concept of the organisation; two-factor authentication is mandatory for HR administrators; encryption in transit and at rest; audit logs for administrative actions.
- **Processing location:** database, authentication and storage at Supabase on AWS eu-central-1 (Frankfurt, Germany).
- **Sub-processor transfers:** Supabase (hosting); Lovable and Cloudflare (application delivery, e-mail).

B.4 Growmino One Members (once made available)

- **Subject matter and purpose:** membership management for sports schools, clubs and associations, including member records, contracts, attendance and communication. This section applies from the date the Module is made available to Customer.
- **Categories of data subjects:** members and prospective members, including minors; parents and legal guardians; trainers and staff; Authorised Users.
- **Categories of Personal Data:** identity and contact data (name, date of birth, postal address, e-mail address, telephone number); data of parents or legal guardians; membership and contract data (tariff, start and end, status, grades or levels); attendance and check-in data; communication data; photos, where uploaded by Customer.
- **Special categories:** health data only in the fields designated for this purpose, and only after a data protection impact assessment has been carried out for the Module. Safeguards: designated fields only; access restricted by role and permission concept; encryption in transit and at rest; audit logs for administrative actions. Customer is responsible for the legal basis, including any explicit consent, and for any consent of parents or legal guardians required for minors.
- **Processing location and Sub-processor transfers:** as stated in Appendix 3 at the time the Module is made available. Provider will announce the hosting region in accordance with Section 6 of the DPA.

B.5 Professional Services

- **Subject matter and purpose:** development of websites and web applications, AI automation, management of Google and Meta advertising, content and AI video production and consulting, in each case as described in the respective SOW, to the extent Provider processes Customer Personal Data.
- **Categories of data subjects:** as defined by the SOW, typically Customer's website visitors, leads and customers, recipients of advertising, persons depicted or heard in

content provided by Customer, and Customer's employees and contact persons.

- **Categories of Personal Data:** as defined by the SOW, typically contact and form data, lead data, advertising audience data within Customer's advertising accounts, usage data of websites operated for Customer, and images, video and voice recordings provided by Customer.
- **Processing location and Sub-processor transfers:** the Sub-processors in Appendix 3 for the respective service and any additional Sub-processor named in the SOW. Customer's own advertising, analytics and integration accounts are Customer-Connected Services. Provider does not upload images, videos or voice recordings of identifiable persons provided by Customer to generative AI services unless the SOW expressly provides for this.

C. Competent supervisory authority (Annex I.C)

The competent supervisory authority is determined under Clause 13 of the SCC as follows: (a) where Customer is established in the EU, the supervisory authority of its establishment; (b) where Customer is not established in the EU but has appointed a representative under Art. 27 GDPR, the supervisory authority of the Member State in which the representative is established; (c) otherwise, the supervisory authority of the Member State in which the data subjects are located. For transfers under the UK Addendum, the UK Information Commissioner; for transfers under the FADP, the FDPIC.

Appendix 2: Technical and Organisational Measures (Annex II to the SCC)

Provider operates the Services as cloud applications on the infrastructure of its Sub-processors. Provider operates no data centres or application servers of its own for the Services. Physical security of the data centres is ensured by the infrastructure Sub-processors. The measures below describe what Provider implements. Provider does not claim certifications of its own (such as ISO/IEC 27001 or SOC 2). Where available, Provider relies on the certifications and audit reports of its Sub-processors.

1. Confidentiality

1.1 **Encryption in transit:** all connections to the Services use TLS 1.2 or higher.

1.2 **Encryption at rest:** data in the database and storage is encrypted at rest by AWS and Supabase using AES-256.

1.3 **Tenant separation:** each customer organisation is logically separated in the database through PostgreSQL Row Level Security (RLS). The RLS policies were verified in a security

review in 2026.

1.4 **Authentication:** two-factor authentication (TOTP) is mandatory for Provider's superadmins and available for Customer administrators. In the HR Module, two-factor authentication is mandatory for administrators.

1.5 **Authorisation:** role and permission concept per organisation; Customer assigns roles to its Authorised Users.

1.6 **Least privilege and secrets:** service keys are granted on a least-privilege basis; secrets are stored and used only on the server side and are not exposed to client applications.

1.7 **Hashing:** PINs for time-recording terminals and API keys are stored only as peppered hashes.

1.8 **Provider access:** Provider accesses Customer Personal Data only to provide support or on Customer's instructions (Section 5.2 of the DPA).

1.9 **Confidentiality of personnel:** all persons with access are bound to confidentiality. Provider is a one-person operation; substitution is governed by the representation arrangement in Provider's operating agreement.

1.10 **No AI training:** Customer Personal Data is not used to train AI models.

2. Integrity

2.1 **Audit logs:** administrative actions are logged.

2.2 **Immutable acceptance records:** acceptances of contract documents (including the Terms and this DPA) are stored in records that cannot be altered.

2.3 **Electronic signature audit trail:** in the Booking Module, signing events (link access, OTP verification, timestamps, IP address, user agent) are recorded in an audit trail.

2.4 **Protection against abuse:** rate limiting and bot protection (honeypot) at registration.

2.5 **Transport integrity:** TLS protects data against alteration in transit.

3. Availability

3.1 **Backups:** daily backups of the database by the database provider (Supabase).

3.2 **Distributed delivery:** application delivery via Cloudflare's global edge network.

3.3 **Monitoring:** monitoring of the Services with alerts.

3.4 **Offline mode:** the HR terminal can record working time offline and synchronises the records once connectivity is restored.

4. Resilience

4.1 **Managed infrastructure:** use of managed database, storage and edge infrastructure of established providers instead of self-operated servers.

4.2 **Incident process:** a defined process for detecting, assessing, containing and reporting security incidents, supported by monitoring and alerts.

4.3 **Continuity of operation:** substitution of the sole operator under the representation arrangement in Provider's operating agreement.

5. Ability to restore availability and access

5.1 Restoration from the daily backups of the database provider.

5.2 Backups are retained for no longer than 90 days after deletion of the data in the production system (Section 10.2 of the DPA).

6. Regular testing, assessment and evaluation

6.1 Review of tenant separation (RLS policies), last verified in a security review in 2026.

6.2 Evaluation of monitoring alerts and of incidents within the incident process.

6.3 Review of the measures in this Appendix when the Services change materially, in particular before new Modules go live.

7. Data minimisation, retention and deletion

7.1 Deletion concept with defined export window and deletion periods (Section 10 of the DPA): 90 days' export after the end of the Agreement, a Subscription or an unconverted Trial, deletion within a further 30 days, backups within 90 days.

7.2 Customer can delete individual records at any time using the functions of the Services.

8. Measures for Sub-processors

8.1 Selection of Sub-processors that provide sufficient guarantees for appropriate technical and organisational measures.

8.2 Contracts meeting the requirements of Art. 28(3) and (4) GDPR and appropriate safeguards for transfers under Chapter V GDPR (DPF certification of the Sub-processor where available, otherwise standard contractual clauses).

8.3 Selection of EU hosting regions for the databases (Frankfurt and Ireland) where offered.

8.4 Review of Sub-processors before engagement and when they materially change their services or terms; notification of changes under Section 6 of the DPA.

9. Measures in relation to government access (Clause 15 of the SCC)

9.1 Hosting of Customer Personal Data in EU regions (Section 8.3), encryption in transit and at rest.

9.2 Review of each request for legality, challenge of unlawful requests, and disclosure only of the minimum data required (Section 12 of the DPA).

9.3 Notification of Customer, unless prohibited, and best efforts to obtain a waiver of any prohibition.

9.4 Documentation of requests, legal assessments and challenges; transparency information to Customer on request.

9.5 No back doors (Section 12.6 of the DPA).

10. Measures for assistance to Customer

10.1 Functions to search, correct, export and delete data to support data subject requests (Section 7 of the DPA).

10.2 Export functions for Customer Data (Section 10.1 of the DPA and Schedule 4 of the Terms).

Appendix 3: Sub-processors (Annex III to the SCC)

The current list of Sub-processors is published at growmino.de/legal/subprocessors. Changes are made in accordance with Section 6 of the DPA. As of the effective date (1 December 2026), Customer authorises the following Sub-processors:

Sub-processor	Service	Modules	Location / region
Supabase Inc. (USA), on Amazon Web Services	Database, authentication, storage	CRM, Booking, HR	CRM: AWS eu-central-1 (Frankfurt, Germany); Booking: AWS eu-west-1 (Ireland); HR: AWS eu-central-1 (Frankfurt, Germany). Support and administrative access from the USA possible

Sub-processor	Service	Modules	Location / region
Lovable Labs Incorporated / Lovable (Sweden)	Application hosting via Cloudflare Workers, build, transactional e-mail via notify.growmino.de, AI Gateway	All Modules	EU, USA, global edge
Cloudflare, Inc. (USA)	CDN, edge execution	All Modules	Global
Google LLC (USA) / Google Ireland Limited (Ireland)	AI models (Gemini) via the Lovable AI Gateway for transcription and text generation	CRM (AI transcription and summaries), Booking (AI offers and texts)	USA, EU
Twilio Inc. (USA)	Telephony, SMS, call recordings and voicemail	CRM (where Provider's telephony is used)	USA
Hostinger International Ltd. (Cyprus), servers in Lithuania	VPS hosting	Professional Services only (websites operated by Provider for Customer under a SOW); no Customer Data from the Growmino One applications	Lithuania, EU
Google Ireland Limited (Ireland) / Google LLC (USA), Google Workspace	Provider's business e-mail, calendar and file storage for support, project communication and file exchange	All Modules and Professional Services	EU, USA

Not Sub-processors: Stripe Payments Europe, Limited and Stripe, Inc. (independent controllers for payments); Customer-Connected Services, including Customer's own Google Workspace, Microsoft 365 and Twilio accounts.