Data Processing Agreement

Version: 1.0
Effective Date: June 30, 2026

This Data Processing Agreement (“DPA”) forms part of the Master Services Agreement, Terms of Service, Order Form, Statement of Work, or other written agreement between:

LeadPipelines:
[LEGAL ENTITY NAME], operating as **LeadPipelines**
[MAILING ADDRESS]
Alberta, Canada
Email: **[legal@leadpipelines.com]**

and

Customer:
[CUSTOMER LEGAL NAME]
[CUSTOMER ADDRESS]
Email: **[CUSTOMER EMAIL]**

LeadPipelines and Customer may each be referred to as a “Party” and together as the “Parties.”

This DPA governs LeadPipelines’ processing of Personal Data on behalf of Customer in connection with LeadPipelines’ CRM, automation, funnel, booking, messaging, payment workflow, and managed service offerings.

---

1. Purpose

The purpose of this DPA is to define the Parties’ privacy, data protection, security, subprocessor, breach notification, data return, and deletion obligations where LeadPipelines processes Personal Data on behalf of Customer.

This DPA is intended to support compliance with applicable privacy and data protection laws, including where applicable:

- Alberta’s Personal Information Protection Act
- Canada’s Personal Information Protection and Electronic Documents Act
- GDPR
- UK GDPR
- Other applicable privacy, data protection, and electronic communications laws

---

2. Definitions

In this DPA:

“Agreement” means the agreement between LeadPipelines and Customer that governs the Services, including any Master Services Agreement, Terms of Service, Order Form, Statement of Work, or related document.

“Applicable Data Protection Laws” means all privacy and data protection laws applicable to the relevant processing of Personal Data.

“Controller” means the party that determines the purposes and means of processing Personal Data. Where applicable, this term includes equivalent concepts such as “business,” “organization,” or “data controller.”

“Customer Data” means data, records, contacts, leads, prospects, CRM entries, form submissions, messages, calendar data, files, campaign data, payment workflow data, notes, tags, call data, and other information submitted to, uploaded to, collected through, or processed by the Services on behalf of Customer.

“Data Subject” means an identified or identifiable individual whose Personal Data is processed.

“Personal Data” means any information relating to an identified or identifiable individual that is processed by LeadPipelines on behalf of Customer through the Services. This includes “personal information” and similar terms under Applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed by LeadPipelines on behalf of Customer.

“Processing” means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, restriction, erasure, or destruction.

“Processor” means the party that processes Personal Data on behalf of a Controller. Where applicable, this term includes equivalent concepts such as “service provider” or “third-party processor.”

“Services” means the CRM setup, funnel setup, automation setup, booking setup, payment workflow setup, email/SMS workflow setup, managed services, software access, support, and related services provided by LeadPipelines.

“Subprocessor” means any third party engaged by LeadPipelines to process Personal Data on behalf of Customer in connection with the Services.

“Third-Party Services” means third-party platforms, vendors, software, APIs, infrastructure, processors, carriers, payment providers, email providers, SMS providers, booking tools, hosting providers, analytics tools, and other external services used with or through the Services.

3. Roles of the Parties

For Personal Data processed by LeadPipelines on behalf of Customer:

- Customer is generally the Controller.
- LeadPipelines is generally the Processor.

Customer determines the purposes and means of processing Personal Data, including what Personal Data is collected, why it is collected, how it is used, which contacts are imported, which messages are sent, which campaigns are run, and which legal bases, notices, consents, and opt-out processes apply.

LeadPipelines processes Personal Data on behalf of Customer only to provide, support, secure, maintain, and improve the Services, or as otherwise permitted by this DPA, the Agreement, Customer's documented instructions, or applicable law.

Some Third-Party Services may act as processors for some purposes and independent controllers or independent service providers for other purposes, including billing, fraud prevention, abuse prevention, security, legal compliance, account administration, analytics, or platform operations.

---

4. Scope of Processing

This DPA applies only to Personal Data processed by LeadPipelines on behalf of Customer in connection with the Services.

This DPA does not apply to:

- Personal Data LeadPipelines processes for its own business purposes as an independent controller;
- Personal Data collected directly by LeadPipelines from website visitors, prospects, or customers for LeadPipelines' own sales, billing, marketing, security, or administrative purposes;
- Personal Data processed directly by Customer outside the Services;
- Personal Data processed by third parties under their own independent terms, unless they act as LeadPipelines' Subprocessors for the Services.

LeadPipelines' handling of Personal Data for its own purposes is described in its Privacy Policy.

---

5. Customer Instructions

Customer instructs LeadPipelines to process Personal Data as reasonably necessary to:

- Provide the Services;
- Configure and maintain CRM systems;
- Build and manage forms, funnels, pipelines, calendars, workflows, and automations;
- Send, receive, route, log, and manage email, SMS, phone, booking, and related communications;

- Import, organize, tag, update, and manage CRM contacts;
- Process payments and payment workflow data where applicable;
- Provide support and troubleshooting;
- Monitor service performance;
- Maintain security;
- Prevent fraud, spam, abuse, and misuse;
- Comply with applicable law;
- Comply with Third-Party Service requirements;
- Enforce the Agreement.

Customer's documented instructions include this DPA, the Agreement, applicable Order Forms, Statements of Work, configuration choices, account settings, written instructions, and Customer's use of the Services.

LeadPipelines may refuse or suspend processing instructions that LeadPipelines reasonably believes violate applicable law, Third-Party Service requirements, security requirements, or acceptable use obligations.

---

6. Customer Obligations

Customer represents and warrants that:

- It has the right to provide Personal Data to LeadPipelines;
- It has provided all required privacy notices;
- It has obtained all required consents;
- It has a valid legal basis for all processing instructions;
- It has the right to use all contacts, leads, lists, forms, campaigns, and messages processed through the Services;
- Its use of the Services complies with Applicable Data Protection Laws;
- Its marketing, SMS, email, phone, and automation activities comply with applicable consent, unsubscribe, and anti-spam requirements;
- It will not upload unlawful, improperly obtained, purchased, rented, scraped, harvested, or prohibited contact lists;
- It will not use the Services for sensitive or regulated data unless approved by LeadPipelines in writing;
- It will maintain proof of consent where required;
- It will honour unsubscribe, STOP, opt-out, do-not-contact, and suppression requests.

Customer is responsible for responding to Data Subject requests where Customer controls the Personal Data.

Customer is responsible for ensuring that its own privacy policies, form notices, consent language, campaign disclosures, SMS disclosures, unsubscribe mechanisms, and end-user communications are accurate and legally compliant.

---

7. LeadPipelines Obligations

LeadPipelines will:

- Process Personal Data only on Customer's documented instructions, unless required by law;
- Use reasonable administrative, technical, and organizational safeguards;
- Limit access to Personal Data to personnel, contractors, advisors, and Subprocessors who need access to provide the Services;
- Ensure authorized personnel are subject to confidentiality obligations;
- Use commercially reasonable efforts to assist Customer with privacy requests, security obligations, breach response, and deletion requests, subject to the limits of the Services;
- Use Subprocessors only as permitted by this DPA;
- Notify Customer of confirmed Personal Data Breaches as described in this DPA;
- Return or delete Personal Data as described in this DPA;
- Maintain reasonable records to demonstrate compliance with this DPA.

LeadPipelines does not provide legal advice and is not responsible for determining whether Customer's instructions, campaigns, messages, contact lists, privacy notices, consents, or legal bases comply with applicable law.

---

8. Confidentiality

LeadPipelines will ensure that personnel authorized to process Personal Data are subject to confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

LeadPipelines will not intentionally disclose Personal Data to unauthorized parties except as permitted by this DPA, the Agreement, Customer's instructions, or applicable law.

---

9. Security Measures

LeadPipelines will implement and maintain reasonable administrative, technical, and organizational measures designed to protect Personal Data against unauthorized access, collection, use, disclosure, copying, modification, disposal, loss, or destruction.

Security measures may include, as appropriate:

- Role-based access controls;
- Password protection;
- Multi-factor authentication where available;
- Secure administrative access;
- Least-privilege access practices;
- Internal access restrictions;
- Logging and monitoring;
- Backup and recovery controls;

- Vendor review;
- Incident response procedures;
- Account offboarding procedures;
- Confidentiality obligations for personnel;
- Reasonable physical, technical, and organizational safeguards;
- Encryption where appropriate and available through the relevant platform or provider.

Customer acknowledges that the Services rely on Third-Party Services and that some security controls are provided by those Third-Party Services.

Customer is responsible for securing its own users, devices, accounts, passwords, domains, DNS, email systems, payment systems, calendars, connected platforms, and administrator access.

No system, transmission, or storage method is completely secure. LeadPipelines does not guarantee absolute security.

---

10. Subprocessors

Customer gives LeadPipelines general authorization to use Subprocessors to provide the Services.

LeadPipelines may use Subprocessors for:

- CRM infrastructure;
- Marketing automation;
- Email delivery;
- SMS and phone services;
- Payment processing;
- Booking and calendar workflows;
- Hosting;
- analytics;
- support;
- security;
- logging;
- backup;
- monitoring;
- professional services;
- other functions reasonably needed to provide the Services.

LeadPipelines will require Subprocessors to process Personal Data under obligations that are materially protective of Personal Data, taking into account the nature of the services provided by the Subprocessor.

LeadPipelines remains responsible for its own obligations under this DPA, subject to the limitations of liability in the Agreement.

---

11. Current Subprocessor List

As of the Effective Date, LeadPipelines may use the following Subprocessors or Third-Party Services, depending on Customer's purchased Services and configuration:

Subprocessor / Provider	Purpose
GoHighLevel / HighLevel	CRM, automation, funnels, forms, workflows, pipelines, calendars, customer account functionality
Twilio	SMS, phone, messaging, carrier services, related communication infrastructure
Mailgun / Sinch	Email delivery and related email infrastructure
Stripe	Payments, billing, subscriptions, fraud prevention, payment workflow records
Calendly or similar booking tool	Appointment booking and calendar scheduling
Domain, DNS, and hosting providers	Website, domain, hosting, routing, and technical infrastructure
Email and workspace providers	Business communications, support, administration
Analytics providers	Website, funnel, and service analytics
Support and communication tools	Customer support, tickets, messages, internal operations
Security, logging, backup, and monitoring tools	Security, diagnostics, backups, availability, and incident response
Professional advisors	Legal, accounting, insurance, compliance, and business advisory services

LeadPipelines may update the Subprocessor list from time to time as its business, vendor stack, or Services change.

---

12. Subprocessor Changes and Objections

LeadPipelines may add, replace, or remove Subprocessors from time to time.

Where required by Applicable Data Protection Laws or by a written enterprise agreement, LeadPipelines will provide notice of material Subprocessor changes.

Customer may object to a new Subprocessor only where Customer has a reasonable, good-faith privacy or security concern.

If Customer objects, the Parties will work in good faith to find a commercially reasonable solution. If no reasonable solution is available, LeadPipelines may terminate the affected Services, and Customer's sole remedy will be a pro-rata refund of prepaid unused fees for the affected Services, if any.

Customer may not object to a Subprocessor solely because it is located outside Customer's jurisdiction if cross-border processing is otherwise permitted under this DPA and applicable law.

---

13. Cross-Border Transfers

Customer acknowledges that Personal Data may be processed, stored, transferred, or accessed in Canada, the United States, and other jurisdictions where LeadPipelines or its Subprocessors operate.

Customer is responsible for ensuring that Customer's use of the Services and transfer of Personal Data to LeadPipelines is lawful.

Where required by Applicable Data Protection Laws, the Parties will use appropriate transfer mechanisms, which may include:

- Adequacy decisions;
- Standard Contractual Clauses;
- UK transfer addendum or equivalent mechanism;
- Data Privacy Framework participation where applicable;
- Contractual safeguards;
- Other lawful transfer mechanisms.

If Standard Contractual Clauses or other transfer terms are required, they will apply only to the extent necessary under Applicable Data Protection Laws and only for the relevant restricted transfer.

If there is a conflict between this DPA and mandatory transfer terms required by Applicable Data Protection Laws, the mandatory transfer terms will control for the relevant transfer.

---

14. Data Subject Requests

Customer is responsible for receiving and responding to Data Subject requests relating to Personal Data processed through the Services.

Data Subject requests may include requests to:

- Access Personal Data;
- Correct Personal Data;
- Delete Personal Data;
- Restrict processing;
- Object to processing;
- Withdraw consent;

- Request portability;
- Opt out of marketing;
- Exercise other rights under Applicable Data Protection Laws.

To the extent LeadPipelines receives a request directly from a Data Subject relating to Personal Data controlled by Customer, LeadPipelines may:

- Refer the requester to Customer;
- Notify Customer of the request;
- Decline to act unless instructed by Customer;
- Respond as required by applicable law.

LeadPipelines will provide commercially reasonable assistance with Data Subject requests where Customer cannot reasonably fulfil the request using the Services.

LeadPipelines may charge reasonable fees for manual, excessive, complex, repetitive, or out-of-scope assistance.

---

15. Opt-Outs, Unsubscribes, and Suppression

Customer is responsible for ensuring that all required unsubscribe, STOP, opt-out, do-not-contact, and suppression processes are implemented and honoured.

LeadPipelines may process opt-out, unsubscribe, STOP, suppression, bounce, complaint, and similar data to:

- Provide the Services;
- Prevent unlawful messaging;
- Maintain suppression lists;
- Comply with provider policies;
- Protect deliverability;
- Prevent abuse;
- Comply with applicable law.

Customer must not remove, bypass, disable, or override suppression controls unless legally authorized and technically supported.

---

16. Personal Data Breach Notification

LeadPipelines will notify Customer without undue delay after confirming a Personal Data Breach involving Personal Data processed by LeadPipelines on behalf of Customer.

The notice will include available information reasonably known to LeadPipelines at the time, which may include:

- Nature of the incident;

- Categories of Personal Data affected;
- Categories or approximate number of affected Data Subjects, if known;
- Likely consequences, if known;
- Measures taken or proposed to address the incident;
- Measures that may reduce possible harm;
- Contact point for follow-up.

LeadPipelines may provide information in phases as investigation continues.

LeadPipelines' notice of a Personal Data Breach is not an admission of fault, liability, or legal responsibility.

Customer is responsible for determining whether notice to Data Subjects, regulators, customers, or other third parties is required.

Customer is responsible for making any required regulator or Data Subject notifications unless LeadPipelines is legally required to do so directly.

---

17. Security Incident Cooperation

The Parties will reasonably cooperate in investigating, mitigating, documenting, and remediating confirmed Personal Data Breaches involving Personal Data.

Customer must promptly notify LeadPipelines if Customer becomes aware of any security incident that may affect the Services, Customer's Account, Customer Data, connected Third-Party Services, or Personal Data processed by LeadPipelines.

Customer is responsible for incidents caused by Customer's users, systems, devices, passwords, credentials, account settings, connected platforms, domains, DNS, payment systems, calendars, campaigns, or misuse of the Services.

---

18. Breach Records

LeadPipelines will maintain reasonable internal records of confirmed Personal Data Breaches involving Personal Data processed by LeadPipelines on behalf of Customer.

These records may include:

- Incident date or discovery date;
- Description of the incident;
- Personal Data involved;
- Affected systems;
- Containment steps;
- Assessment notes;
- Notification decisions;

- Remediation steps.

Records will be retained as required by applicable law and LeadPipelines' internal retention practices.

---

19. Assistance With Compliance

Taking into account the nature of the Services and information available to LeadPipelines, LeadPipelines will provide commercially reasonable assistance to Customer with:

- Security obligations;
- Personal Data Breach assessments;
- Data Subject requests;
- Data protection impact assessments;
- transfer impact assessments;
- regulator inquiries;
- audit questionnaires;
- deletion or export requests.

Assistance is limited to the Personal Data processed by LeadPipelines on behalf of Customer through the Services.

LeadPipelines may charge reasonable fees for assistance that is manual, excessive, complex, repetitive, urgent, outside ordinary support scope, or required because of Customer's use case, instructions, or non-compliance.

---

20. Audits and Information Requests

Upon reasonable written request, LeadPipelines may provide information reasonably necessary to demonstrate compliance with this DPA.

LeadPipelines may satisfy audit or information requests by providing:

- Written responses;
- Security summaries;
- Vendor documentation;
- Subprocessor information;
- Policy summaries;
- Compliance questionnaires;
- Certifications or reports if available;
- Other reasonable documentation.

Customer may not conduct onsite audits unless required by Applicable Data Protection Laws and only if:

- Customer gives reasonable prior written notice;
- The audit is limited to relevant processing under this DPA;

- The audit does not compromise security, confidentiality, or other customers' information;
- The audit occurs during normal business hours;
- The audit is subject to confidentiality obligations;
- Customer pays reasonable costs associated with the audit;
- The audit is not duplicative of available documentation.

No audit may require LeadPipelines to disclose trade secrets, confidential third-party information, internal security details that would increase risk, or information relating to other customers.

---

21. Sensitive Data

The Services are not designed for sensitive, regulated, or special-category data unless LeadPipelines expressly agrees in writing.

Customer must not upload, collect, process, or transmit the following through the Services without LeadPipelines' prior written approval:

- Health information;
- Financial account information;
- Government identification numbers;
- Children's information;
- Biometric information;
- Criminal record information;
- Precise location data;
- Special-category personal data;
- Payment card data outside approved payment processor workflows;
- Other data requiring heightened legal protection.

Customer is responsible for ensuring that any approved sensitive-data use case is lawful and technically supported by the relevant Third-Party Services.

LeadPipelines may suspend or terminate any use case that creates unacceptable legal, privacy, security, vendor, carrier, payment, or operational risk.

---

22. Return and Deletion of Personal Data

Upon termination of the Services or upon Customer's written instruction, LeadPipelines will delete or return Personal Data where reasonably possible, subject to:

- Technical limitations;
- Backup cycles;
- Legal obligations;
- accounting, tax, billing, fraud-prevention, and dispute-resolution requirements;
- Security and abuse-prevention requirements;
- Third-Party Service retention practices;

- Compliance records;
- Suppression and opt-out records;
- Aggregated, anonymized, or de-identified information;
- Information retained by Customer or exported before termination.

Customer is responsible for exporting Personal Data before cancellation or termination where export functionality is available.

LeadPipelines is not responsible for loss of Personal Data after termination, suspension, non-payment, account closure, vendor deletion, or Customer's failure to export data.

---

23. Backup and Residual Copies

Personal Data may remain in backups, logs, archives, or residual copies for a limited period after deletion from active systems.

LeadPipelines will delete or overwrite backup and residual copies according to ordinary backup cycles, vendor practices, technical limitations, and legal retention obligations.

LeadPipelines is not required to delete Personal Data from backups immediately if doing so is technically impractical or would compromise security, integrity, disaster recovery, or legal obligations.

---

24. De-Identified and Aggregated Data

LeadPipelines may create and use aggregated, anonymized, or de-identified data for analytics, benchmarking, reporting, service improvement, security, training, and business purposes, provided the data does not identify Customer or any individual.

LeadPipelines will not attempt to re-identify de-identified data except as permitted by applicable law.

---

25. Government and Legal Requests

If LeadPipelines receives a subpoena, court order, regulator request, law enforcement request, or other legal demand for Personal Data processed on behalf of Customer, LeadPipelines may notify Customer unless legally prohibited.

LeadPipelines may disclose Personal Data where required by law.

LeadPipelines will use reasonable efforts to limit disclosure to what is legally required, taking into account the nature of the request, legal obligations, urgency, and available information.

Customer is responsible for responding to legal requests directed to Customer.

26. Third-Party Service Terms

Customer acknowledges that the Services depend on Third-Party Services that may have their own privacy, security, data processing, acceptable use, messaging, payment, retention, and compliance terms.

Customer's use of the Services may be affected by Third-Party Service requirements, including requirements imposed by:

- GoHighLevel / HighLevel;
- Twilio;
- Mailgun / Sinch;
- Stripe;
- Calendly;
- carriers;
- email providers;
- payment processors;
- hosting providers;
- other vendors.

LeadPipelines is not responsible for Third-Party Service changes, suspensions, outages, enforcement actions, retention practices, or independent processing activities.

---

27. Marketing and Messaging Compliance

Customer is solely responsible for determining whether its marketing, SMS, email, phone, booking, review request, reminder, and automation activities are lawful.

Customer must ensure that:

- It has required consent or another valid legal basis;
- It can prove consent where required;
- Its contact lists are lawfully collected;
- Its messages identify the sender where required;
- Its messages include unsubscribe or opt-out mechanisms where required;
- STOP, unsubscribe, opt-out, do-not-contact, and suppression requests are honoured;
- It does not send spam, misleading claims, fraudulent messages, or prohibited content;
- It does not use purchased, rented, scraped, harvested, or unlawful contact lists where prohibited.

LeadPipelines may suspend or restrict processing where Customer's messaging activity creates legal, compliance, provider, carrier, deliverability, payment, reputational, or operational risk.

---

28. Limitation of Liability

The limitation of liability, exclusions of damages, indemnities, disclaimers, and liability carve-outs in the Agreement apply to this DPA.

This DPA does not increase LeadPipelines' total liability beyond the amounts stated in the Agreement unless expressly stated otherwise in a signed written agreement.

Customer's liability for unlawful instructions, unlawful contact lists, unlawful marketing, consent failures, privacy violations, Customer Data, Customer Content, and End User claims is governed by the Agreement.

---

29. Conflict

If there is a conflict between this DPA and the Agreement regarding processing of Personal Data, this DPA controls for that processing issue.

If there is a conflict between this DPA and mandatory data transfer terms required by Applicable Data Protection Laws, the mandatory transfer terms control for the relevant transfer.

All other commercial, payment, service, warranty, indemnity, liability, dispute, and termination terms remain governed by the Agreement.

---

30. Term

This DPA begins when LeadPipelines first processes Personal Data on behalf of Customer and continues until LeadPipelines no longer processes Personal Data on behalf of Customer, subject to any surviving obligations.

Sections that by their nature should survive termination will survive, including confidentiality, security, deletion, residual copies, government requests, limitation of liability, and conflict terms.

---

31. Changes to This DPA

LeadPipelines may update this DPA from time to time to reflect changes in law, Third-Party Services, security practices, business operations, or the Services.

Where required by law or by a written enterprise agreement, LeadPipelines will provide notice of material changes.

Customer's continued use of the Services after an updated DPA becomes effective means Customer accepts the updated DPA.

Schedule 1 — Processing Details

1. Subject Matter

LeadPipelines processes Personal Data on behalf of Customer to provide CRM setup, funnel setup, form setup, automation setup, booking workflows, payment workflows, email/SMS workflows, managed services, support, troubleshooting, and related services.

2. Duration

Processing continues for the term of the Agreement and any applicable Order Form or SOW, plus any period required for backups, deletion, legal retention, dispute resolution, compliance, billing, security, or transition.

3. Nature of Processing

Processing may include:

- Collection;
- Recording;
- Organization;
- Structuring;
- Storage;
- Hosting;
- Accessing;
- Importing;
- Exporting;
- Copying;
- Transmission;
- Retrieval;
- Consultation;
- Use;
- Modification;
- Tagging;
- Segmentation;
- Automation;
- Messaging;
- Booking;
- Support;
- Troubleshooting;
- Logging;
- Backup;
- Deletion.

4. Purpose of Processing

The purpose of processing is to provide the Services, including:

- CRM setup and operation;
- Contact and lead management;
- Form and funnel operation;
- Pipeline setup;
- Workflow automation;
- Email and SMS communication;
- Missed-call text-back functionality;
- Appointment booking;
- Payment workflow support;
- Reporting;
- Customer support;
- Security and abuse prevention;
- Service maintenance and improvement;
- Compliance with law and provider requirements.

5. Categories of Data Subjects

Personal Data may relate to:

- Customer’s leads;
- Customer’s prospects;
- Customer’s customers;
- Customer’s website visitors;
- Customer’s form submitters;
- Customer’s message recipients;
- Customer’s appointment bookers;
- Customer’s staff and contractors;
- Customer’s CRM users;
- Other individuals whose Personal Data is submitted to or processed through the Services.

6. Categories of Personal Data

Personal Data may include:

- Name;
- Email address;
- Phone number;
- Business name;
- Job title or role;
- Address or service area;
- Website URL;
- Form submissions;
- CRM records;

- Tags and notes;
- Pipeline status;
- Appointment and calendar information;
- Email content;
- SMS content;
- Communication history;
- Call-related metadata where applicable;
- Consent records;
- Opt-in and opt-out records;
- Unsubscribe records;
- Suppression records;
- Payment workflow metadata;
- IP address;
- Device and browser information;
- Usage and activity logs;
- Other information submitted by Customer or End Users through the Services.

7. Sensitive Data

Sensitive data is not permitted unless expressly approved in writing by LeadPipelines.

Schedule 2 — Technical and Organizational Measures

LeadPipelines will maintain reasonable technical and organizational measures appropriate for its stage of business, the Services provided, and the nature of the Personal Data.

Measures may include:

1. Access Control

- Role-based access where available;
- Least-privilege access practices;
- Access limited to personnel and contractors with a business need;
- Removal of access when no longer required;
- Administrative access controls.

2. Authentication

- Password-protected systems;
- Multi-factor authentication where available;
- Secure account access practices;
- Credential access limited to authorized personnel.

3. System Security

- Use of reputable Third-Party Services;
- Vendor security review where appropriate;
- Secure administrative access;
- Monitoring of suspicious activity where available;
- Reasonable malware, abuse, and unauthorized-access prevention practices.

4. Data Handling

- Personal Data used only as needed to provide the Services;
- Customer Data separated by customer account or platform configuration where available;
- Suppression and opt-out data handled to prevent unlawful messaging;
- Data exports and deletions handled according to available platform functionality.

5. Backups and Recovery

- Backup and recovery controls through applicable platforms and vendors;
- Reasonable efforts to maintain continuity of service;
- Deletion subject to backup cycles and vendor practices.

6. Incident Response

- Internal incident escalation process;
- Investigation and containment steps;
- Customer notification process for confirmed Personal Data Breaches;
- Documentation of confirmed incidents.

7. Confidentiality

- Confidentiality obligations for personnel, contractors, advisors, and service providers with access to Personal Data;
- Access limited to those with a need to know.

8. Subprocessor Management

- Use of Subprocessors reasonably necessary to provide the Services;
- Subprocessor obligations materially protective of Personal Data;
- Subprocessor list maintained and updated as needed.

9. Customer Responsibilities

Customer is responsible for:

- Securing its own users and devices;
- Managing its own passwords and credentials;

- Controlling administrator access;
- Maintaining lawful contact lists;
- Maintaining accurate privacy notices and consent records;
- Reviewing and approving automations before launch;
- Exporting Customer Data before termination where needed.

Schedule 3 — Subprocessor List

The following Subprocessors or Third-Party Services may process Personal Data depending on Customer's configuration and purchased Services:

Provider	Purpose	Possible Processing Location
GoHighLevel / HighLevel	CRM, funnels, forms, workflows, automations, calendars, pipelines, account management	Canada, United States, or other provider locations
Twilio	SMS, phone, messaging, telecom, carrier infrastructure	United States or other provider locations
Mailgun / Sinch	Email delivery and email infrastructure	United States, EU, or other provider locations
Stripe	Payments, billing, subscriptions, fraud prevention, payment records	Canada, United States, EU, or other provider locations
Calendly or similar booking provider	Calendar booking and appointment scheduling	United States or other provider locations
Domain, DNS, and hosting providers	Website, domain, routing, hosting, and technical infrastructure	Canada, United States, or other provider locations
Email/workspace providers	Business communications, administration, and support	Canada, United States, or other provider locations
Analytics providers	Website, funnel, and service analytics	Canada, United States, or other provider locations
Support and communication tools	Support requests, customer communications, internal operations	Canada, United States, or other provider locations
Security, backup, logging, and monitoring tools	Security, diagnostics, backups, monitoring, incident response	Canada, United States, or other provider locations
Professional advisors	Legal, accounting, insurance, compliance, and business advisory support	Canada or other applicable locations

LeadPipelines may update this list as its vendor stack changes.

Schedule 4 — Optional EU / UK Transfer Terms Placeholder

This Schedule applies only where required by GDPR, UK GDPR, or other applicable transfer laws.

Where Personal Data is transferred from the European Economic Area, United Kingdom, Switzerland, or another jurisdiction that requires a specific transfer mechanism, the Parties will use an appropriate legal transfer mechanism.

This may include:

- EU Standard Contractual Clauses;
- UK International Data Transfer Addendum;
- UK International Data Transfer Agreement;
- Swiss transfer terms;
- Adequacy decision;
- Data Privacy Framework certification where applicable;
- Another lawful transfer mechanism.

If required, the Parties will complete and attach the applicable transfer documents.

Until completed, this DPA is not intended to replace any mandatory transfer documents required by law.

Signature Page

The Parties agree to this Data Processing Agreement as of the Effective Date.

LeadPipelines
[LEGAL ENTITY NAME]

By: _____
Name: _____
Title: ____
Date: _____

Customer
[CUSTOMER LEGAL NAME]

By: _____
Name: _____

Title: ___
Date: _____