

# Privacy Policy

**Effective Date:** June 30, 2026

**Last Updated:** June 30, 2026

LeadPipelines (“LeadPipelines,” “we,” “us,” or “our”) respects your privacy. This Privacy Policy explains how we collect, use, disclose, store, and protect personal information when you visit our website, contact us, use our services, interact with our forms, or use CRM, automation, marketing, booking, payment, and related services provided by us.

This Privacy Policy applies to LeadPipelines’ website, landing pages, forms, customer portals, CRM setup services, automation services, email and SMS workflows, booking integrations, payment workflows, and related business services.

For purposes of this Privacy Policy, “personal information” means information about an identifiable individual.

LeadPipelines is operated by [LEGAL ENTITY NAME], located in **Alberta, Canada**.

Contact: [privacy@leadpipelines.com]

---

## 1. What LeadPipelines Does

LeadPipelines provides CRM setup, marketing automation, funnel setup, lead intake systems, missed-call text-back systems, booking workflows, payment workflows, email/SMS automation, and related managed services for businesses.

Our services may involve third-party platforms and service providers, including but not limited to GoHighLevel / HighLevel, Twilio, Mailgun / Sinch, Stripe, Calendly, website hosting providers, analytics tools, and support tools.

---

## 2. Scope of This Policy

This Privacy Policy applies to personal information we collect and handle in three main situations:

- 1. Website and marketing visitors**

People who visit our website, complete our forms, book calls, request information, or communicate with us.

- 2. Customers and customer users**

Businesses and their staff who purchase, access, or manage LeadPipelines services.

### **3. Customer lead and CRM data**

Personal information that our customers provide to us or collect through systems we build, manage, or support, including CRM contacts, leads, prospects, form submissions, SMS replies, email replies, booking information, and related automation data.

Where we process personal information on behalf of a business customer, that customer is generally responsible for deciding what information is collected, why it is collected, how it is used, and whether the required notices, consents, legal bases, and unsubscribe processes are in place.

---

## **3. Personal Information We Collect**

We may collect the following types of personal information.

### **A. Information You Provide Directly**

This may include:

- Name
- Email address
- Phone number
- Business name
- Job title or role
- Website URL
- Business address or service area
- Information submitted through website forms
- Information provided during sales calls, onboarding calls, or support conversations
- Billing and subscription information
- Communications with us
- Files, brand assets, copy, campaign details, or business information you provide to us

### **B. Website, Device, and Usage Information**

When you visit our website or interact with our online services, we may collect:

- IP address
- Browser type
- Device type
- Operating system
- Pages viewed
- Referring website
- Approximate location based on IP address
- Date and time of visits
- Form interaction data
- Cookie and analytics information
- Other technical information used to operate, secure, and improve our website

## **C. Customer Account and CRM Information**

When a customer uses LeadPipelines services, we may process:

- Customer account details
- Admin and user login details
- CRM contacts and lead records
- Form submissions
- Pipeline activity
- Appointment and calendar information
- Email and SMS communication history
- Call-related metadata where applicable
- Automation activity
- Tags, notes, tasks, opportunities, and workflow data
- Consent, opt-in, opt-out, unsubscribe, and suppression data
- Support requests and troubleshooting records

## **D. Payment Information**

We may collect payment-related information such as:

- Billing name
- Billing email
- Billing address
- Subscription status
- Invoice history
- Payment status
- Transaction identifiers

Payments may be processed through Stripe or another payment provider. We do not intend to store full credit card numbers on our own systems.

## **E. Communications and Messaging Data**

If you communicate with us or use systems we provide, we may process:

- Emails
  - SMS messages
  - Form messages
  - Support messages
  - Booking confirmations
  - Automation messages
  - Replies, opt-outs, unsubscribes, and suppression events
-

## 4. How We Use Personal Information

We may use personal information to:

- Provide our services
  - Build, configure, manage, and support CRM systems
  - Set up landing pages, forms, booking flows, automations, email workflows, and SMS workflows
  - Process payments, subscriptions, invoices, and billing records
  - Communicate with customers and prospects
  - Respond to inquiries and support requests
  - Book calls and manage appointments
  - Send service updates, onboarding information, and administrative messages
  - Send marketing communications where permitted by law
  - Maintain unsubscribe, opt-out, and suppression lists
  - Monitor platform performance and troubleshoot issues
  - Improve our website, services, templates, workflows, and customer experience
  - Protect against fraud, spam, misuse, unauthorized access, security threats, and policy violations
  - Comply with legal, regulatory, tax, accounting, and contractual obligations
  - Enforce our agreements, policies, and acceptable use requirements
  - Create aggregated or de-identified information that does not identify an individual
- 

## 5. Customer Responsibility for Contact Lists, Leads, and Campaigns

Customers are responsible for the personal information they provide to LeadPipelines or collect through systems we build, configure, or manage for them.

Customers are responsible for ensuring that:

- Their contact lists are lawfully collected
- They have the required consents, permissions, or legal bases to contact individuals
- Their forms, funnels, landing pages, campaigns, and messages comply with applicable laws
- Their email, SMS, calling, and marketing activities comply with applicable laws
- Their messages include required sender identification and unsubscribe options where required
- Opt-outs, STOP requests, unsubscribe requests, and suppression lists are honoured
- They do not upload purchased, rented, scraped, or otherwise unlawful contact lists
- They do not use LeadPipelines services to send spam, unlawful messages, misleading content, or prohibited content

LeadPipelines may suspend, restrict, or terminate services where we believe a customer is using the services unlawfully, abusively, or in a way that creates risk for LeadPipelines, our vendors, carriers, payment processors, or other customers.

---

## 6. Consent and Marketing Communications

We may send marketing communications to individuals who have consented to receive them or where we are otherwise permitted by law.

Marketing communications may include emails, SMS messages, updates, promotions, service information, and related business communications.

Where required, commercial electronic messages will include sender identification and an unsubscribe mechanism.

You may unsubscribe from our marketing emails by using the unsubscribe link in the email or by contacting us at [[privacy@leadpipelines.com](mailto:privacy@leadpipelines.com)].

You may opt out of SMS messages by replying **STOP**, where supported, or by contacting us.

Even if you unsubscribe from marketing messages, we may still send non-marketing messages, such as service notices, billing notices, security notices, legal notices, account updates, or responses to your inquiries.

---

## 7. Cookies and Analytics

We may use cookies, pixels, tags, analytics tools, and similar technologies to operate our website, understand how visitors use our website, improve our marketing, and measure the performance of our pages and campaigns.

These technologies may collect information such as:

- IP address
- Device type
- Browser type
- Pages viewed
- Time spent on pages
- Referring links
- Form activity
- Advertising or campaign interaction data

You can control cookies through your browser settings. Some website features may not function properly if cookies are disabled.

If we use non-essential analytics, advertising pixels, retargeting tools, or similar tracking technologies in jurisdictions that require opt-in consent, we will use reasonable efforts to provide the required consent mechanism.

---

## 8. Third-Party Service Providers

We may use third-party service providers to operate our business and provide our services. These providers may process personal information on our behalf or, in some cases, act as independent controllers or independent service providers for certain purposes.

These providers may include:

- GoHighLevel / HighLevel for CRM, automation, funnels, forms, workflows, and customer management
- Twilio for SMS, phone, messaging, and related communication services
- Mailgun / Sinch for email delivery and related email infrastructure
- Stripe for payment processing, billing, subscriptions, fraud prevention, and payment records
- Calendly or similar tools for appointment booking
- Website hosting providers
- Domain, DNS, and email infrastructure providers
- Analytics and tracking providers
- Customer support and communication tools
- Security, logging, backup, and monitoring tools
- Professional advisors, including lawyers, accountants, insurers, and consultants

We require service providers to handle personal information appropriately and only as needed to provide services, comply with law, prevent abuse, maintain security, or perform their contractual obligations.

---

## 9. When We Disclose Personal Information

We may disclose personal information:

- To service providers that help us operate our business
- To platforms and infrastructure providers needed to deliver our services
- To payment processors for billing and subscription management
- To communication providers for SMS, email, phone, and related services
- To calendar and booking providers
- To contractors, employees, or advisors who need access to provide services
- To comply with legal obligations, court orders, subpoenas, regulatory requests, or lawful government requests
- To investigate, prevent, or respond to fraud, abuse, spam, security incidents, or unlawful activity
- To enforce our agreements, policies, and rights
- In connection with a business transaction, such as a merger, acquisition, financing, reorganization, or sale of assets
- With your consent or at your direction

We do not sell personal information in the ordinary course of business.

---

## 10. Cross-Border Processing

LeadPipelines is based in Alberta, Canada. However, personal information may be processed, stored, accessed, or transferred in Canada, the United States, and other jurisdictions where we or our service providers operate.

Privacy laws in those jurisdictions may differ from the laws in your province, state, or country. Personal information may also be subject to lawful access requests by courts, law enforcement, national security authorities, or regulators in those jurisdictions.

By using our website or services, or by providing personal information to us, you understand that personal information may be processed outside your jurisdiction.

---

## 11. Data Retention

We retain personal information only as long as reasonably necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law.

Retention periods may depend on:

- The type of information
- The purpose for collection
- Customer account status
- Legal, tax, accounting, and billing requirements
- Contractual requirements
- Security, fraud prevention, and abuse-prevention needs
- Backup and disaster recovery processes
- Dispute resolution or enforcement needs

Customer CRM data may remain in active systems, backups, logs, archives, or vendor systems for a limited period after termination, subject to technical limitations, legal requirements, contractual requirements, and backup deletion cycles.

Customers are responsible for exporting their data before cancellation or termination where export is available and required.

---

## 12. Security

We use reasonable administrative, technical, and organizational safeguards designed to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, modification, and destruction.

These safeguards may include:

- Access controls

- Password protection
- Role-based permissions
- Multi-factor authentication where available
- Encryption where appropriate
- Secure administrative access
- Logging and monitoring
- Vendor review
- Backup and recovery controls
- Internal access restrictions
- Incident response procedures

No system, transmission, or storage method is completely secure. We cannot guarantee absolute security.

Customers are responsible for managing their own users, passwords, permissions, administrator access, connected accounts, imported data, and campaign activity.

---

### **13. Privacy Breaches and Security Incidents**

If we become aware of a privacy breach or security incident involving personal information under our control, we will assess the incident and take reasonable steps to contain, investigate, document, and remediate it.

Where required by applicable law, we will notify affected individuals, customers, regulators, or other required parties.

Where we process personal information on behalf of a customer, we may notify the affected customer so the customer can assess and satisfy its own legal obligations.

---

### **14. Access, Correction, and Privacy Requests**

Subject to applicable law, you may request access to personal information we hold about you or request that we correct inaccurate personal information.

You may also request that we delete certain personal information, withdraw consent where processing is based on consent, or stop using your information for certain purposes, subject to legal, contractual, security, technical, and business limitations.

To make a privacy request, contact:

**[[privacy@leadpipelines.com](mailto:privacy@leadpipelines.com)]**

We may need to verify your identity before responding.

If your information is held by one of our business customers through a CRM, form, funnel, or automation we provide to that customer, we may direct your request to that customer because the customer is generally responsible for deciding how that information is handled.

---

## **15. International Privacy Rights**

Depending on where you live, you may have additional privacy rights under local law.

These rights may include the right to:

- Access your personal information
- Correct inaccurate information
- Request deletion
- Restrict or object to processing
- Request portability
- Withdraw consent
- Object to direct marketing
- File a complaint with a privacy regulator

We will respond to applicable privacy requests as required by law.

If you are located in the European Economic Area, United Kingdom, or another jurisdiction with similar privacy laws, LeadPipelines may process your information based on one or more lawful bases, including contract performance, consent, legal obligations, legitimate interests, or your direction through a customer-controlled service.

---

## **16. Children's Information**

Our services are intended for businesses and are not directed to children.

We do not knowingly collect personal information from children. Customers must not use our services to collect information from children unless they have the legal authority to do so and have entered into any required additional written agreement with us.

---

## **17. Sensitive Information**

Our services are not designed for highly sensitive personal information unless we expressly agree otherwise in writing.

Customers must not upload, collect, or process sensitive information through LeadPipelines services unless they have confirmed that the use case is lawful, appropriate, and supported by the relevant third-party platforms.

Sensitive information may include health information, financial account information, government identification numbers, children’s information, biometric information, precise location information, or other information requiring special legal protection.

---

## 18. Customer Websites, Forms, and Funnels

Where LeadPipelines builds or manages a website, landing page, form, funnel, calendar, or automation for a customer, the customer is responsible for ensuring that its own privacy policy, terms, consent language, marketing disclosures, SMS disclosures, and unsubscribe processes are accurate and legally compliant.

LeadPipelines may provide templates, setup support, or technical implementation, but customers remain responsible for approving their own legal notices, campaign content, contact lists, and consent language.

---

## 19. Links to Other Websites

Our website and services may contain links to third-party websites, platforms, integrations, or tools.

We are not responsible for the privacy practices, content, policies, or security of third-party websites or services. You should review the privacy policies of any third-party services you use.

---

## 20. Changes to This Privacy Policy

We may update this Privacy Policy from time to time.

When we update it, we will revise the “Last Updated” date above. The updated version will be effective when posted unless stated otherwise.

Your continued use of our website or services after an updated Privacy Policy is posted means you acknowledge the updated policy.

---

## 21. Contact Us

For privacy questions, requests, or complaints, contact:

**LeadPipelines**

**[LEGAL ENTITY NAME]**

**[MAILING ADDRESS]**

**Alberta, Canada**

**Email:** [privacy@leadpipelines.com]

**Website:** https://leadpipelines.com