

PRIVACY POLICY

Effective Date: April 7, 2026

Compliance: PIPEDA | CASL | Provincial Privacy Laws

1. Introduction and Our Commitment to Privacy

This Privacy Policy explains how Stryde ("Company") collects, uses, discloses, retains, and protects personal information in connection with this website and our digital marketing and AI automation services (collectively, the "Services").

We are committed to protecting your privacy and handling your personal information responsibly in compliance with Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA), applicable provincial privacy legislation, and Canada's Anti-Spam Legislation (CASL).

By accessing our website or using our Services, you consent to the collection, use, and disclosure of your personal information as described in this Privacy Policy.

2. Scope of This Policy

This Privacy Policy applies to:

- All personal information collected through this website
- Personal information collected through contact forms, lead generation forms, and newsletter signups
- Personal information collected in connection with providing our Services to clients
- Personal information collected through email communications and marketing campaigns
- Personal information processed through AI automation tools and workflows

This Policy does not apply to the practices of third-party companies whose websites may be linked from our site, or to third-party tools and platforms we use, which are governed by their own privacy policies.

3. Personal Information We Collect

3.1 Information You Provide Directly

We may collect the following personal information that you voluntarily provide to us:

- Contact information: name, email address, phone number, mailing address
- Business information: company name, job title, industry, website URL

- Account credentials: username and password (if applicable)
- Communication content: messages sent through our contact forms or email
- Marketing preferences: communication opt-ins, frequency preferences, topic interests
- Payment information: billing address, payment card details (processed securely through third-party payment processors — we do not store full card numbers)
- Client-provided data: any data, assets, or materials you provide for the purpose of receiving our Services

3.2 Information We Collect Automatically

When you visit our website, we may automatically collect:

- Device and technical data: IP address, browser type and version, operating system, device identifiers
- Usage data: pages visited, time spent on pages, referring URLs, click-stream data
- Location data: general geographic location inferred from IP address
- Cookie and tracking data: session cookies, persistent cookies, pixel tags (see Section 8 for details)

3.3 Information from Third Parties

We may receive personal information about you from:

- Social media platforms (if you interact with our social media accounts or connect via social login)
- Advertising platforms (audience data for ad targeting and retargeting)
- CRM systems and marketing tools integrated with our Services
- Data enrichment services used to supplement client contact lists
- Referral sources (if a third party refers you to us)

4. How We Use Your Personal Information

We collect and use personal information only for purposes that a reasonable person would consider appropriate in the circumstances, and only with your knowledge and consent as required by PIPEDA. Our purposes include:

4.1 Providing and Improving Services

- Delivering the digital marketing and AI automation services you have requested
- Processing transactions and managing client accounts
- Communicating with you about your account or Service engagements
- Personalizing and improving our Services and website experience
- Developing, testing, and improving our AI automation systems

4.2 Marketing and Communications

- Sending commercial electronic messages (CEMs) with your express or implied consent under CASL
- Delivering newsletters, marketing updates, and promotional content
- Conducting surveys and gathering feedback
- Notifying you of new services, features, or offers that may interest you

4.3 Legal and Compliance Purposes

- Complying with applicable legal obligations and regulatory requirements
- Responding to lawful requests from government authorities
- Establishing, exercising, or defending legal claims
- Detecting, investigating, and preventing fraud or other illegal activity

4.4 Analytics and Business Operations

- Analyzing website traffic and usage patterns
- Measuring the effectiveness of marketing campaigns
- Generating internal reports and business analytics
- Maintaining the security and integrity of our systems

5. Consent and Legal Basis for Processing

Under PIPEDA, we rely on the following bases for collecting and using your personal information:

- **Express Consent:** For marketing emails and direct communications, we obtain your explicit opt-in consent. You may withdraw consent at any time (see Section 10).
- **Implied Consent:** Where PIPEDA permits, we may rely on implied consent, such as when an existing business relationship exists or your contact information has been conspicuously published.
- **Contractual Necessity:** To fulfill our obligations under a Service Agreement with you or your organization.
- **Legal Obligation:** Where required by Canadian federal or provincial law.
- **Legitimate Interests:** For limited purposes such as fraud prevention and network security, where your interests and fundamental rights do not override our legitimate interests.

You may withdraw your consent at any time, subject to legal or contractual restrictions. Withdrawal of consent may affect our ability to provide certain Services. To withdraw consent, please contact our Privacy Officer (see Section 14).

6. Disclosure of Personal Information

6.1 Service Providers

We may share personal information with trusted third-party service providers who assist us in operating our business and providing the Services, including:

- Cloud hosting and infrastructure providers
- Email marketing platforms (e.g., Mailchimp, HubSpot, ActiveCampaign)
- CRM systems and sales platforms
- AI and machine learning platforms (e.g., OpenAI, Google AI)
- Payment processors
- Analytics and advertising platforms (e.g., Google Analytics, Meta Business Suite)
- Professional advisors (lawyers, accountants, auditors)

We require all service providers to maintain appropriate privacy and security standards and to use personal information only for the specific purpose of providing services to us.

6.2 Legal Disclosures

We may disclose personal information when required by law, court order, or lawful government authority, or when we believe disclosure is necessary to protect our rights, your safety, or the safety of others.

6.3 Business Transactions

In the event of a merger, acquisition, restructuring, or sale of all or part of our business, personal information may be transferred to the acquiring entity, subject to equivalent privacy protections.

6.4 No Sale of Personal Information

We do not sell, rent, or trade your personal information to third parties for their own marketing purposes.

7. International Data Transfers

Some of our service providers and technology platforms are located outside of Canada, including in the United States. When we transfer personal information outside Canada, we take contractual and other measures to ensure that your information receives a comparable level of protection as it does under PIPEDA.

By using our Services, you acknowledge and consent to the transfer of your personal information to countries outside Canada. Where required by applicable law, we will provide specific notice of cross-border transfers.

8. Cookies and Tracking Technologies

8.1 Types of Cookies We Use

- **Essential Cookies:** Required for the website to function properly. These cannot be disabled.
- **Analytics Cookies:** Used to understand how visitors interact with our website (e.g., Google Analytics). Data collected is aggregated and anonymized where possible.
- **Marketing and Advertising Cookies:** Used to deliver relevant advertisements and track campaign performance across platforms including Google Ads and Meta Ads.
- **Functional Cookies:** Remember your preferences and settings to improve your experience.

8.2 Pixel Tags and Web Beacons

We and our advertising partners may use pixel tags and web beacons on our website and in our emails to track engagement, measure campaign performance, and facilitate ad retargeting.

8.3 Your Cookie Choices

Most web browsers allow you to control cookie settings. You can set your browser to refuse cookies or alert you when cookies are being sent. Note that disabling cookies may affect your ability to use certain features of our website. You may also opt out of interest-based advertising through the Digital Advertising Alliance of Canada (DAAC) at youradchoices.ca.

9. Retention of Personal Information

We retain personal information only for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required or permitted by law. Our general retention guidelines are:

- **Client data:** Retained for the duration of the Service relationship plus 7 years for tax and accounting purposes, or as required by applicable law
- **Marketing contact data:** Retained until you unsubscribe or withdraw consent, with records of consent retained as required by CASL
- **Website analytics data:** Typically retained for 26 months in aggregate form
- **Communication records:** Retained for 3 years from the date of last communication
- **Legal and compliance records:** Retained as required by applicable law

When personal information is no longer required, we securely destroy, delete, or anonymize it in accordance with our data retention procedures.

10. Your Privacy Rights

Under PIPEDA and applicable provincial privacy law, you have the following rights with respect to your personal information:

10.1 Right of Access

You have the right to request access to the personal information we hold about you, including information about how it has been used and to whom it has been disclosed. We will respond to access requests within 30 days, or provide notice if an extension is required.

10.2 Right to Correction

If you believe personal information, we hold about you is inaccurate, incomplete, or out-of-date, you may request that we correct or update it.

10.3 Right to Withdraw Consent

You may withdraw your consent to our collection, use, or disclosure of your personal information at any time, subject to legal or contractual restrictions. Withdrawal may limit our ability to provide certain Services.

10.4 Right to Unsubscribe (CASL)

Every commercial electronic message we send includes a clear and functional unsubscribe mechanism. You may opt out of receiving marketing emails at any time. We will process unsubscribe requests within 10 business days as required by CASL.

11. Privacy and AI Automation Services

Our AI Automation Services involve the use of personal data in automated workflows. The following applies specifically to AI-related data processing:

- **Data Minimization:** We use only the minimum personal information necessary to achieve the automation objective.
- **No Automated Decision-Making with Legal Effect:** We do not use automated systems to make decisions that have significant legal or similarly significant effects on individuals without human review.
- **AI Platform Data Practices:** When using third-party AI platforms to process personal data, we execute Data Processing Agreements (DPAs) with such providers where required. Personal data submitted to AI APIs is subject to the privacy practices of those platforms.
- **Model Training:** We do not use your confidential client data to train AI models without your explicit written consent.
- **Transparency:** We will inform you if your personal information is subject to any automated profiling or AI-driven segmentation as part of our Services.

12. Data Security

We implement industry-standard technical, administrative, and physical safeguards to protect personal information against unauthorized access, use, disclosure, alteration, and destruction. Our security measures include:

- Encryption of personal data in transit (TLS/SSL) and at rest where appropriate
- Role-based access controls limiting access to personal information on a need-to-know basis
- Regular security assessments and vulnerability testing
- Employee training on privacy and data security obligations
- Secure disposal of personal information when no longer needed
- Incident response procedures for data breaches

In the event of a breach of security safeguards involving personal information that poses a real risk of significant harm, we will notify affected individuals and the Office of the Privacy Commissioner of Canada as required by PIPEDA's mandatory breach notification requirements.

13. Children's Privacy

Our Services are not directed to individuals under the age of 18. We do not knowingly collect personal information from minors. If we become aware that we have inadvertently collected personal information from a person under 18, we will take immediate steps to delete it. If you believe we may have collected information from a minor, please contact our Privacy Officer immediately.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. We will indicate the effective date of any updates at the top of this Policy.

Where required by applicable law or where changes are material, we will notify you by email or by posting a prominent notice on our website before the changes take effect. Your continued use of the Services after the effective date of the revised Policy constitutes your acceptance of the changes.

15. Contact Our Privacy Team

If you have any questions, concerns, or complaints about this Privacy Policy or our privacy practices, or to exercise your privacy rights, please contact our designated Privacy Team:

Company: Stryde

Address: Toronto, ON, Canada

Email: support.stryde@gmail.com

Phone: (647) 829-3778

We will acknowledge your request within 5 business days and respond fully within 30 days, or as required by applicable law.

Your privacy matters to us. We are committed to protecting your personal information and being transparent about how we use it.