PRIVACY POLICY

PayVia Payments Corp.

Licensed Money Service Business (MSB) — FINTRAC Licence No. M20883922

Effective Date: [Insert Date] | Last Updated: [Insert Date]

1. Overview

PayVia Payments Corp. ("PayVia," "we," "us," or "our") is a company incorporated in Canada (company number BC1263699), with its registered office at 666 Burrard Street, Suite 652, Vancouver, BC V6C 2X8, Canada. PayVia is registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a Money Service Business (MSB) under Licence No. M20883922, pursuant to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

As a federally regulated MSB under PCMLTFA, PayVia is required to report certain financial transactions to FINTRAC without client consent and without notifying the client. This includes Suspicious Transaction Reports (STRs) and Large Cash Transaction Reports (LCTRs). If a suspicious transaction report is filed in relation to your account, you will not be notified of such filing. These disclosures are mandatory under Canadian law and do not require your consent.

We have developed this Privacy Policy ("Policy") in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) to explain how we collect, use, process, store, share, and transfer your personal data through our services and via our website at www.payvia.net (the "Website").

We are committed to protecting and respecting your privacy. This Policy describes the personal data we collect, how we use it, with whom we share it, your rights and choices, and how you can contact us about our privacy practices.

This Policy, together with our Terms and Conditions and Cookie Policy, sets out the basis on which we process any personal data we collect from you or that you provide to us. Please read it carefully.

Scope: This Policy applies only to personal data collected by PayVia. It does not apply to any third-party websites, products, or services, even if they link to our Website or services.

Consent Mechanisms: We obtain your consent to collect and use personal data in the following ways: (a) **Express consent** — provided actively by you at the time of onboarding, account opening, or KYC verification, through checkbox acceptance, digital signature, or written acknowledgement of this Policy; and (b) **Implied consent** — reasonably inferred from your use of our Website or services (e.g., voluntarily providing information or navigating our platform). Where required by law or where the purpose of processing is not evident from context, we will seek express consent. You may withdraw consent at any time, subject to legal and contractual restrictions, by contacting us at the details set out in Section 17.

"You" and "your" in this Policy refer to any visitor or user of our Website and/or user of our services.

2. Regulatory Compliance

PayVia is committed to full compliance with the following legislation and regulatory frameworks:

- The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal private-sector privacy law.
- British Columbia's Personal Information Protection Act (PIPA).
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), as administered by FINTRAC.
- Canada's Anti-Spam Legislation (CASL), governing commercial electronic messages.

3. Information You Provide to Us

You may provide personal data to us in various ways, including by completing forms on our Website, applying to open an account, subscribing to our services, contacting us by phone, email, or through our mobile application, or reporting an issue.

A. Individual Applicants/Clients

- Full legal name
- Date of birth
- Photograph or video for identity verification
- Residential address with proof (e.g., utility bill or bank statement)
- Government-issued identification details (e.g., passport, national ID), including images
- Employment information (job title, employer)
- Contact details (email address, phone number)

B. Corporate Clients (Legal Entities)

For shareholders holding more than 10% control or ownership, directors, and authorized signatories ("Authorized Representatives"), we require the information listed in Section A above, plus:

- Curriculum vitae (CV) of each shareholder, director, and Authorized Representative
- Description of the business and its partners
- Full set of corporate documentation (certificates of incorporation, licences, resolutions) required for applicant and representative identification
- Business contact details (email, phone, website)

We reserve the right to request financial statements and any additional information we deem necessary to provide our services.

Your Responsibility: By submitting an application, you confirm that you are authorized to disclose the personal data provided and that you have obtained all necessary consents from the individuals whose data you supply. PayVia is not liable for any claim arising from your failure to ensure the lawful transfer of personal data to us.

4. Information We Collect Automatically

When you visit our Website, we may automatically collect the following types of information:

- Technical data: Internet Protocol (IP) address, login credentials, browser type and version, browser plug-in types and versions, operating system, device type, and platform.
- Usage data: Uniform Resource Locators (URLs) of pages visited, clickstream data to, through, and from our Website; products, services, or other content viewed or searched for; page response times, interaction statistics and logs (including errors), navigation methods, and any phone number used to contact us.

We may also collect information about your online activity on our Website and connected devices over time and across third-party websites, applications, and services.

5. Cookies

Our Website uses cookies and similar tracking technologies to distinguish you from other users. This helps us provide a better browsing experience and allows us to improve our Website. For detailed information on the cookies we use and the purposes for which we use them, please refer to our Cookie Policy.

6. How We Use Your Information

Information You Provide

We use this information to:

- Evaluate your applications, provide the services set out in our agreements with you, and respond to your requests for information, products, or services.
- Enable fraud protection and risk management, including screening against third-party sanctions lists and other relevant databases to confirm your eligibility for our services.
- Conduct third-party screening and sanctions checks as part of our risk-based AML/CTF compliance framework. This includes screening your personal data against: (i) sanctions lists maintained by regulatory bodies such as the Office of the Superintendent of Financial Institutions (OSFI) and the United Nations Security Council; (ii) Politically Exposed Persons (PEPs) databases; and (iii) adverse media

sources. Such screening is conducted on an ongoing basis and is required for the purpose of complying with our obligations under PCMLTFA and related FINTRAC guidance.

- Monitor, prevent, and detect unauthorized payment transactions.
- Comply with our legal and regulatory obligations.
- Respond to enquiries, issue service notices, and provide customer support.
- Inform you about products and services similar to those you have purchased or enquired about.
- With your consent, provide you with information about other products or services that may interest you.
- Notify you of changes to our services.
- Ensure that Website content is presented in the most effective manner for you.

Information We Collect Automatically

We use this information to:

- Administer and maintain our Website, including troubleshooting, testing, research, and data analysis.
- Improve Website content and presentation.
- Maintain Website security.
- Measure the effectiveness of advertising and deliver relevant content to you.
- Make recommendations about products or services that may interest you.

7. Disclosure of Your Information

We may share your personal data with the following parties:

- Group companies: Affiliated companies, subsidiaries, and parent entities as defined under applicable law.
- Service providers and business partners: Subcontractors and third-party providers engaged to perform contractual obligations or fulfil regulatory requirements on our behalf.
- Analytics and search engine providers: Partners that assist us in improving and optimizing our Website.

We may also disclose your personal data in the following circumstances:

- Where required by law, regulation, or court order, or to enforce our Terms and Conditions or other agreements.
- To protect the rights, property, or safety of PayVia, our clients, business partners, or others, including for the purposes of fraud prevention and credit risk reduction.
- In response to lawful requests from courts, law enforcement, regulatory agencies, or other public authorities, including authorities outside your country of residence.

- In connection with a sale, merger, acquisition, or other transfer of business assets, in which case your personal data may be disclosed to the prospective buyer, subject to appropriate confidentiality protections.

8. Data Storage & Retention

PayVia maintains reasonable administrative, technical, and physical security measures to protect your personal data against loss, misuse, unauthorized access, disclosure, and alteration. These measures include firewalls, data encryption, access authorization controls, and physical access restrictions at our data centres. Access to your personal data is limited to personnel who require it to perform their duties.

You are responsible for maintaining the confidentiality of your password(s) and account credentials, and for verifying that any personal data we hold about you is accurate and up to date. We strongly advise you not to share your password with anyone. If you believe the security of your account has been compromised, please contact us immediately.

While we strive to protect your personal data, no method of transmission over the Internet is completely secure. Any transmission of data to our Website is at your own risk.

Retention Periods

We retain your personal data for as long as we are providing services to you and for such additional period as necessary to:

- Comply with our legal and regulatory obligations, including tax, accounting, and financial reporting requirements.
- Conduct fraud monitoring, detection, and prevention.
- Fulfil contractual commitments with our partners.
- Satisfy retention requirements mandated by the payment methods we support or applicable law.
- **Minimum 5-year retention for AML/KYC records:** In accordance with PCMLTFA and FINTRAC requirements, we retain all AML/KYC-related records — including identity verification documents, transaction records, and risk assessments — for a minimum of five (5) years following account closure or the date of the last transaction, whichever is later. This mandatory retention period applies regardless of any earlier request by you to delete or erase your personal data.

We implement retention schedules aligned with applicable legal and regulatory requirements and periodically review retained data to confirm continued necessity.

9. Legal Basis for Processing

We process your personal data on one or more of the following legal bases:

- **Meaningful consent (PIPEDA Principle 3):** We rely on your knowledge and consent for the collection, use, or disclosure of your personal data, except where otherwise required or permitted by law. Consent may be express or implied

depending on the sensitivity of the information and the reasonable expectations of the individual. We make reasonable efforts to ensure that the purpose of collection is clearly communicated so that consent is meaningful and informed.

- **Contractual necessity:** Where processing is necessary to perform a contract with you or to take steps at your request prior to entering into a contract.
- **Legal obligation (no consent required):** Where processing is necessary to comply with a legal or regulatory obligation to which we are subject (e.g., PCMLTFA, PIPEDA, CASL), consent is not required. This includes mandatory disclosures to FINTRAC and other regulatory authorities.
- **Business purposes without consent (PIPEDA Schedule 1, Clause 4.3.4):** In limited circumstances permitted under PIPEDA, we may collect, use, or disclose personal data without consent where it is clearly in the individual's interest and consent cannot be obtained in a timely way, or where seeking consent would compromise the availability or accuracy of the information (e.g., fraud investigation).

10. Your Rights

Subject to applicable law and regulatory obligations, you have the following rights in relation to your personal data:

- Right of access: You may request confirmation of whether we process your personal data and obtain a copy of that data.
- Right to rectification: You may request correction of personal data that is inaccurate, incomplete, or outdated.
- Right to erasure: You may request deletion of your personal data in certain circumstances provided by law.
- Right to restrict processing: You may request that we restrict the use of your personal data in certain circumstances.
- Right to data portability: You may request that we export your personal data to another organization, where technically feasible.
- Right to object: You may object to the processing of your personal data on grounds relating to your particular situation.
- Right to withdraw consent: Where processing is based on your consent, you may withdraw that consent at any time, without affecting the lawfulness of processing carried out prior to withdrawal.

To exercise any of these rights, please contact us using the details in the Contact Us section below. We will respond to your request as soon as reasonably practicable and to the extent permitted by applicable law. For your protection, we may need to verify your identity before processing your request.

Any access request may be subject to a reasonable fee to cover our administrative costs, as permitted by applicable law.

Updating Your Account Information

We encourage you to review, correct, and update your personal data regularly to keep it current. You may do so by signing in to your PayVia account or by contacting us directly.

Breach Notification

In the event of a breach of security safeguards involving your personal data, PayVia will take the following steps in accordance with PIPEDA's breach of security safeguards regulations:

- **Notification to affected individuals:** Where a breach creates a real risk of significant harm to an individual (including bodily harm, humiliation, damage to reputation or relationships, loss of employment, financial loss, identity theft, or negative effects on a credit record), we will notify affected individuals as soon as feasible.
- **Reporting to the Office of the Privacy Commissioner of Canada:** Where a breach poses a real risk of significant harm, we will report the breach to the Office of the Privacy Commissioner of Canada as required by law, and maintain records of all breaches of security safeguards for a minimum of 24 months from the date we determine a breach has occurred.
- **Notification to other organizations:** Where another organization may be able to reduce the risk of harm or mitigate harm that has occurred, we will notify that organization of the breach.

11. Opting Out of Electronic Communications

If you no longer wish to receive marketing communications from us, you may opt out by using the unsubscribe link included in any marketing email we send you, or by contacting us directly.

Please note that even if you opt out of marketing communications, we may still send you transactional messages and service-related notices that are necessary to provide our services or to comply with legal and regulatory obligations.

12. International Data Transfers

As a global business, we may transfer your personal data to countries other than the one in which it was originally collected. These countries may have data protection laws that differ from those in your jurisdiction.

Processing Outside Canada: Your personal data may be stored, processed, or accessed in countries outside of Canada, including but not limited to the United States and other jurisdictions where our service providers, technology partners, or affiliated entities operate. By using our services, you acknowledge that your personal data may be transferred to and processed in these jurisdictions.

Foreign Government Access: When your personal data is processed outside Canada, it may be subject to access by foreign governments, courts, law enforcement, or regulatory authorities under the laws of those jurisdictions. Such access may occur without notice to

you and without your consent, including under national security, anti-money laundering, or other public-interest legislation applicable in those jurisdictions. PayVia will take reasonable contractual and organizational measures to protect your data, but cannot guarantee the same level of protection as Canadian law in all circumstances.

Where we transfer personal data internationally, we take appropriate measures to ensure that such transfers comply with applicable data protection laws and that your personal data remains protected to the standards described in this Policy. These measures may include contractual safeguards such as standard contractual clauses or reliance on adequacy decisions.

In certain circumstances, courts, law enforcement agencies, regulatory authorities, or security agencies in those countries may be entitled to access your personal data in accordance with local law.

13. Children's Privacy

Our services are not directed at individuals under the age of 18. We do not knowingly collect personal data from children. If we become aware that we have inadvertently collected personal data from a child, we will take prompt steps to delete such data. If you believe we may have collected information from a minor, please contact us immediately.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. Any changes will be posted on this page with an updated "Last Updated" date. Where changes are material, we will notify you by email or by means of a prominent notice on our Website prior to the change becoming effective.

We encourage you to review this Policy periodically to stay informed about how we protect your personal data.

15. Use of Personal Information for AML/CTF Compliance

As a federally registered Money Service Business (MSB), PayVia's use of personal data for anti-money laundering (AML) and counter-terrorist financing (CTF) compliance is a core operational function, not merely incidental processing. The following activities are conducted using your personal data as required by PCMLTFA and associated FINTRAC guidance:

- **Identity verification:** We collect and verify your identity using government-issued identification and other documentation as required by FINTRAC's Know Your Client (KYC) rules. This includes verification at onboarding and on an ongoing basis as required by our risk-based approach.

- **Transaction monitoring:** We monitor your transactions on an ongoing basis to detect patterns or activities that may indicate money laundering, terrorist financing, or other financial crimes. Automated and manual monitoring systems may flag transactions for further review.
- **Risk profiling:** We assess and assign a risk rating to your account based on factors such as your identity, transaction behaviour, geographic exposure, and business type. Risk profiles are reviewed and updated periodically as part of our ongoing due diligence obligations.
- **Reporting obligations:** Where required by law, we will file reports with FINTRAC, including Suspicious Transaction Reports (STRs), Large Cash Transaction Reports (LCTRs), Electronic Funds Transfer Reports (EFTRs), and Casino Disbursement Reports, without your consent and without notifying you of such filing.

The above activities are conducted as a legal obligation and do not require your consent. They cannot be opted out of as a condition of receiving our services.

15. Links to Other Websites

Our Website may contain links to websites operated by our partner networks, advertisers, and affiliates. These websites have their own privacy policies, and we do not accept any responsibility or liability for their content or practices. We encourage you to review the privacy policies of any third-party websites before submitting your personal data.

16. Data Controller

The data controller responsible for your personal data is:

Depending on the nature of the services provided and the relationship between PayVia and its clients and partners, PayVia may act in one or more of the following capacities:

- **Data Controller (direct clients):** Where PayVia collects and processes personal data directly from individual or corporate clients for the purpose of providing payment services and fulfilling its regulatory obligations, PayVia acts as the data controller. In this capacity, PayVia determines the purposes and means of processing personal data and is directly accountable to you under PIPEDA.
- **Data Processor (partners and merchants):** Where PayVia processes personal data on behalf of a business partner, merchant, or third-party platform as part of a service arrangement, PayVia may act as a data processor. In this capacity, PayVia processes personal data only on the instructions of the relevant controller, and the controller retains primary responsibility for compliance with applicable privacy law. Individuals whose data is processed in this context should also review the privacy policy of the relevant partner or merchant.

If you are unsure in which capacity PayVia is acting in relation to your personal data, please contact us using the details in Section 17 below.

PayVia Payments Corp.

Company Number: BC1263699

666 Burrard Street, Suite 652, Vancouver, BC V6C 2X8, Canada

17. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

PayVia Payments Corp.

666 Burrard Street, Suite 652, Vancouver, BC V6C 2X8, Canada

Email: info@payvia.net

If you are not satisfied with our response, you have the right to file a complaint with the Office of the Privacy Commissioner of Canada (www.priv.gc.ca).