



PRIVACY POLICY

Protection of Personal Information

CruisePay Finance Ltd
Effective Date: March 2026

TABLE OF CONTENTS

1. Introduction	3
2. Definitions	3
3. Information We Collect	3
3.1 Information You Provide Directly	3
3.2 Information Collected Automatically	4
3.3 Information from Third Parties	4
4. How We Use Your Information	4
4.1 Service Delivery	4
4.2 Legal and Regulatory Compliance.....	4
4.3 Risk Management and Fraud Prevention	4
4.4 Business Operations	5
5. Legal Basis for Processing	5
6. Disclosure of Personal Information	5
6.1 Regulatory and Law Enforcement Authorities	5
6.2 Financial Institution Partners	5
6.3 Third-Party Service Providers	5
6.4 International Transfers	5
7. Data Retention	6
8. Your Rights	6
8.1 Under PIPEDA / PIPA.....	6
8.2 Under GDPR (for EEA/UK Data Subjects)	6
8.3 Limitations	6
9. Data Security	6
10. Data Breach Notification	7
11. Children's Privacy	7
12. Third-Party Links.....	7
13. Changes to This Privacy Policy	7
14. Contact Information	7

1. Introduction

CruisePay Finance Ltd (“CruisePay,” “we,” “our,” or “us”) is committed to protecting the privacy and security of the personal information of our clients, website visitors, and all individuals whose information we process. This Privacy Policy explains how we collect, use, disclose, retain, and protect your personal information in connection with our payment services, including electronic funds transfers, SEPA transfers, payment card issuance, digital wallet services, and crypto asset exchange services.

This Policy is prepared in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA), British Columbia’s Personal Information Protection Act (PIPA), and, to the extent applicable to our SEPA and European clients, the General Data Protection Regulation (EU GDPR / UK GDPR). Where our obligations under the PCMLTFA require the collection, use, or disclosure of personal information, those obligations prevail as permitted under PIPEDA.

By using our services or providing your personal information to us, you acknowledge that you have read and understood this Privacy Policy.

2. Definitions

- “Personal Information” means information about an identifiable individual, including but not limited to name, address, date of birth, identification documents, financial information, transaction history, and device/usage data.
- “Sensitive Personal Information” means personal information that, by its nature, could cause significant harm if disclosed, including government-issued identification numbers, financial account details, and biometric data.
- “Processing” means any operation performed on personal information, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.
- “Data Subject” means the individual to whom the personal information relates.

3. Information We Collect

3.1 Information You Provide Directly

Account Registration and Identity Verification

- Full legal name, date of birth, and gender.
- Residential and/or business address.
- Email address, phone number, and other contact details.
- Government-issued photo identification (passport, driver’s license, national ID card).
- Proof of address documentation (utility bills, bank statements).
- Occupation, employer name, and source of wealth/funds.
- Tax residency and tax identification numbers.

Entity Client Information

- Corporate registration details, articles of incorporation, and business licenses.
- Beneficial ownership information (names, addresses, dates of birth, and identification of individuals who own or control 25% or more of the entity).

- Authorized signatory information.
- Directors' and officers' details.

Transaction Information

- Originator and beneficiary details for all transfers (EFT, SEPA, crypto).
- Transaction amounts, currencies, dates, and reference numbers.
- Payment card transaction details (merchant, location, amount).
- Crypto asset wallet addresses, transaction hashes, and blockchain data.
- Purpose and reason for transactions.

3.2 Information Collected Automatically

- IP address, browser type, operating system, and device identifiers.
- Log data including pages visited, time spent, links clicked, and referring URLs.
- Cookies and similar tracking technologies (see our Cookie Policy).
- Geolocation data derived from IP address or device settings.

3.3 Information from Third Parties

- Identity verification and fraud prevention providers.
- Credit reference agencies and public registries.
- Sanctions and PEP screening databases.
- Blockchain analytics providers (for crypto asset transactions).
- Correspondent banks and payment network participants.

4. How We Use Your Information

4.1 Service Delivery

- Processing and executing your transactions (EFTs, SEPA transfers, card transactions, crypto exchanges).
- Opening, maintaining, and administering your Account.
- Issuing and managing payment cards.
- Providing customer support and responding to inquiries.

4.2 Legal and Regulatory Compliance

- Verifying your identity as required by the PCMLTFA and FINTRAC guidelines.
- Conducting ongoing monitoring for suspicious transactions.
- Screening against sanctions lists, PEP databases, and terrorist designations.
- Submitting regulatory reports to FINTRAC (STRs, EFT reports, LVCTRs, TPRs).
- Complying with court orders, subpoenas, and law enforcement requests.
- Meeting tax reporting obligations.

4.3 Risk Management and Fraud Prevention

- Conducting risk assessments and assigning client risk ratings.

- Detecting and preventing fraud, unauthorized access, and other security threats.
- Monitoring card usage patterns and crypto transaction flows for anomalies.
- Blockchain analytics to identify connections to sanctioned or illicit addresses.

4.4 Business Operations

- Internal auditing and compliance program reviews.
- Product development and service improvement.
- Statistical analysis and reporting (using aggregated, de-identified data).

5. Legal Basis for Processing

We process your personal information on the following legal bases:

- Contractual necessity: Processing is necessary to perform our contract with you (providing our services).
- Legal obligation: Processing is necessary to comply with the PCMLTFA, FINTRAC guidelines, tax law, and other applicable legislation.
- Legitimate interests: Processing is necessary for fraud prevention, risk management, security, and business operations, where these interests are not overridden by your rights.
- Consent: Where required by applicable law, we obtain your consent before processing. You may withdraw consent at any time, subject to legal and contractual restrictions.

6. Disclosure of Personal Information

We may disclose your personal information to the following categories of recipients:

6.1 Regulatory and Law Enforcement Authorities

CruisePay is required to disclose information to FINTRAC, the RCMP, CSIS, and other law enforcement or regulatory bodies as mandated by the PCMLTFA and other applicable laws. CruisePay is prohibited from notifying you when a suspicious transaction report has been filed.

6.2 Financial Institution Partners

We share originator and beneficiary information with correspondent banks, payment processors, card networks, and SEPA scheme participants as necessary to process your transactions.

6.3 Third-Party Service Providers

We engage service providers who process personal information on our behalf, including: identity verification and KYC providers; blockchain analytics providers; cloud hosting and data storage providers; customer support platforms; and fraud detection services. All service providers are contractually bound to protect your information and to process it only as instructed by CruisePay.

6.4 International Transfers

Your personal information may be transferred to and processed in jurisdictions outside Canada, including within the European Economic Area (for SEPA transactions) and other jurisdictions where our

service providers or correspondents operate. Where such transfers occur, we ensure that appropriate safeguards are in place, including contractual clauses, adequacy decisions, or other mechanisms recognized under applicable law.

7. Data Retention

We retain your personal information for the following minimum periods:

- Client identification records: at least 5 years from the date of the last transaction or the date the business relationship ended, whichever is later.
- Transaction records: at least 5 years from the date the transaction was conducted.
- Regulatory reports (STRs, EFT reports, LVCTRs): at least 5 years from the date of submission to FINTRAC.
- Beneficial ownership records: at least 5 years from the date the business relationship ended.
- Account and communication records: at least 5 years from Account closure.

Information may be retained beyond these minimum periods where required by applicable law, for the resolution of disputes, or to enforce our agreements.

8. Your Rights

8.1 Under PIPEDA / PIPA

- Right to access your personal information held by CruisePay.
- Right to request correction of inaccurate or incomplete information.
- Right to withdraw consent, subject to legal and contractual limitations.
- Right to file a complaint with the Office of the Privacy Commissioner of Canada.

8.2 Under GDPR (for EEA/UK Data Subjects)

If you are located in the European Economic Area or the United Kingdom, you additionally have the right to: request erasure of your personal data (subject to legal retention obligations); restrict processing in certain circumstances; data portability; and object to processing based on legitimate interests. To exercise these rights, contact our Privacy Officer at the address below.

8.3 Limitations

Certain rights may be limited where CruisePay is required by law to retain or process information, including obligations under the PCMLTFA. We cannot disclose information about regulatory reports or compliance investigations.

9. Data Security

CruisePay implements appropriate technical and organizational measures to protect your personal information against unauthorized access, alteration, disclosure, or destruction. These measures include: encryption of data in transit (TLS) and at rest; access controls and role-based permissions; multi-factor authentication for systems containing personal information; regular security assessments and penetration testing; employee training on data protection and information security; and incident response procedures for data breaches.

10. Data Breach Notification

In the event of a data breach that creates a real risk of significant harm, CruisePay will notify affected individuals and the Office of the Privacy Commissioner of Canada as soon as feasible, in accordance with PIPEDA. Where GDPR applies, notification will be made to the relevant supervisory authority within 72 hours of becoming aware of the breach.

11. Children's Privacy

Our services are not intended for individuals under the age of 18 (or the age of majority in their jurisdiction). We do not knowingly collect personal information from minors. If we become aware that we have collected information from a minor, we will take steps to delete it.

12. Third-Party Links

Our platform may contain links to third-party websites or services. CruisePay is not responsible for the privacy practices of these third parties. We encourage you to review their privacy policies before providing any personal information.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Material changes will be communicated to you via email or through our platform at least 30 days before they take effect. The "Effective Date" at the top of this document indicates the most recent revision.

14. Contact Information

If you have questions about this Privacy Policy, wish to exercise your privacy rights, or wish to file a complaint, please contact:

Privacy Officer, CruisePay Finance Ltd

44322 YALE RD UNIT 3B #180 CHILLIWACK, BC, CANADA V2R 4H1

Email: privacy@cruisePay.com

Phone: +44 7455 706040

You may also contact the Office of the Privacy Commissioner of Canada at: <https://www.priv.gc.ca>