PRIVACY POLICY

CEPHEUS PAYMENT CORP
(trading as "Cepheus" and/or "Cepheus Pay")

Last updated: 10 April 2026
Version: 1.1

1. ABOUT THIS PRIVACY POLICY

Cepheus Payment CORP ("**Cepheus**", "**we**", "**us**", "**our**", or the "**Company**") is committed to protecting personal information and handling it responsibly, transparently, and in accordance with applicable privacy laws.

This Privacy Policy explains how we collect, use, disclose, store, protect, and otherwise process personal information in connection with:

- our website(s);
- mobile applications;
- payment, transfer, card, and related services;
- onboarding, verification, and compliance processes;
- communications and business relationships.

This Privacy Policy applies to clients, prospective clients, authorised users, beneficial owners, directors, officers, representatives, business contacts, website visitors, and any other individuals whose personal information we process in connection with our services.

2. WHO WE ARE

Cepheus Payment CORP is a company incorporated under the laws of Canada.

The Company is registered as a **Money Services Business** with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") and is registered as a **Payment Service Provider** with the Bank of Canada under the **Retail Payment Activities Act** ("RPAA"), where applicable. Such registrations do not constitute endorsement, certification, or guarantee by any regulator.

For the purposes of applicable privacy law, Cepheus Payment CORP is generally the organisation responsible for the personal information it collects and controls in connection with its services.

3. PERSONAL INFORMATION WE COLLECT

Depending on the relationship and services involved, we may collect the following categories of personal information.

3.1 Identity and contact information

- full name;
- date of birth;
- nationality or citizenship;
- residential address;
- business address;
- email address;
- telephone number;
- tax identification or similar identifiers, where required.

3.2 Verification and compliance information

- government-issued identification details;
- copies of identity documents;
- proof of address;
- corporate records and registration documents;
- information relating to directors, officers, shareholders, authorised signatories, and beneficial owners;
- source of funds and source of wealth information;
- politically exposed person, sanctions, and adverse media screening results;
- information required for AML / ATF, fraud prevention, and compliance monitoring.

3.3 Financial and transaction information

- payment instructions;
- bank account and settlement details;
- transaction history;
- transfer counterparties;
- balance and ledger information;
- payout information;
- chargeback, dispute, and return data.

3.4 Card-related information

Where card services are provided through our partners, we may process information relating to:

- card issuance and activation;
- card programme participation;
- card transaction information;

- tokenised card data and masked card identifiers;
- card status and usage data.

We do not necessarily receive full card data in all cases, and certain card details may be processed by the Card Issuer or Card Programme Partner instead.

3.5 Technical and usage information

- IP address;
- device identifiers;
- browser type;
- operating system;
- login details;
- session and access logs;
- security and fraud signals;
- website, app, and platform interaction data.

3.6 Communications and support information

- emails;
- chat or support communications;
- call notes;
- complaints and dispute records;
- records of instructions, confirmations, and acknowledgements.

3.7 Marketing and business relationship information

- communication preferences;
- event participation;
- business contact details;
- responses to outreach and marketing communications, where permitted by law.

4. HOW WE COLLECT PERSONAL INFORMATION

We may collect personal information:

4.1 Directly from you

For example, when you:

- apply for services;
- open or use an account;
- submit onboarding materials;
- communicate with us;
- request support;
- use cards or payment functionality;
- respond to compliance or verification requests.

4.2 From third parties

For example, from:

- verification and KYC providers;
- sanctions and screening databases;
- fraud prevention providers;
- banking and payment partners;
- card issuers and card programme partners;
- corporate registries and public records;
- business partners and introducers;
- service providers and technology vendors;
- regulators, authorities, or law enforcement where applicable.

4.3 Automatically

When you use our website, mobile application, or platform, we may automatically collect technical and usage data through cookies, logs, security tools, and analytics technologies.

5. WHY WE COLLECT AND USE PERSONAL INFORMATION

We collect, use, and disclose personal information for purposes that are reasonable and appropriate in the circumstances, including the following.

5.1 To provide services

- open and maintain client relationships;
- authenticate users;
- enable payments, transfers, payouts, and card-related services;
- process instructions and transactions;
- provide support and account management.

5.2 To conduct onboarding and compliance

- verify identity and authority;
- screen against sanctions, PEP, and adverse media data;
- assess eligibility and risk;
- comply with AML / ATF, sanctions, fraud prevention, and related obligations;
- monitor ongoing client activity.

5.3 To protect our business, clients, and partners

- detect, prevent, and investigate fraud, misuse, and unauthorised activity;
- maintain platform and account security;
- manage operational and cyber risks;
- respond to disputes, complaints, and incidents.

5.4 To operate and improve our business

- administer systems and records;

- conduct internal reporting, analytics, and service improvement;
- test, monitor, and improve systems, products, controls, and workflows.

5.5 To communicate with you

- provide service notices and updates;
- respond to questions and requests;
- send compliance reminders;
- deliver marketing or business communications where permitted by applicable law.

5.6 To comply with legal and regulatory obligations

- respond to lawful requests from regulators, courts, law enforcement, banks, processors, and card partners;
- maintain records;
- support examinations, audits, and investigations;
- comply with FINTRAC, RPAA, sanctions, tax, and other legal obligations.

PIPEDA governs collection, use, and disclosure of personal information for purposes that a reasonable person would consider appropriate in the circumstances.

6. CONSENT AND OTHER LEGAL BASES

Where required by applicable law, we obtain consent to collect, use, or disclose personal information. Consent may be express or implied depending on the sensitivity of the information and the circumstances.

In addition, we may process personal information where permitted or required by law, including where necessary to:

- provide requested services;
- comply with legal or regulatory obligations;
- investigate a breach of an agreement or law;
- detect or prevent fraud or financial crime;
- protect our rights, business, clients, employees, or partners.

By applying for, accessing, or using the Services, you acknowledge and agree that we may process personal information as described in this Privacy Policy and in related product or onboarding documentation, subject to applicable law.

You may withdraw consent in certain circumstances, but this may limit or prevent our ability to provide services or continue the relationship.

6A. INTERNATIONAL DATA PROTECTION

The Company primarily operates under Canadian data protection laws, including the **Personal Information Protection and Electronic Documents Act** (“PIPEDA”).

The Company does not actively market or direct its Canadian services to individuals located in the **European Economic Area** (“EEA”) or the **United Kingdom**.

However, where individuals located in such jurisdictions independently access or use the Services, including through unsolicited contact, referral, or word of mouth, the Company may process personal data relating to such individuals.

To the extent that applicable data protection laws of the EEA or the United Kingdom are deemed to apply to specific processing activities, the Company will take commercially reasonable steps to align those activities with the relevant principles of such laws, including, where appropriate:

- identifying a lawful basis for processing;
- implementing appropriate data protection safeguards;
- respecting applicable data subject rights to the extent required by law;
- using lawful transfer mechanisms where cross-border transfer rules apply.

Nothing in this Privacy Policy shall be interpreted as a representation that the Company is subject to, or fully compliant with, GDPR or UK GDPR in all circumstances.

7. DISCLOSURE OF PERSONAL INFORMATION

We may disclose personal information on a need-to-know basis to the following categories of recipients.

7.1 Within our corporate group

We may share information with affiliates and group entities for compliance, fraud prevention, risk management, operational support, and service delivery.

7.2 Service providers and infrastructure partners

We may share information with:

- KYC / AML providers;
- screening and fraud vendors;
- cloud and IT providers;
- analytics and communications providers;
- banking partners;
- payment processors;
- card issuers;
- card programme partners;
- settlement and routing partners.

7.3 Regulators, authorities, and law enforcement

We may disclose information where required or permitted by law to:

- FINTRAC;
- the Bank of Canada;
- courts and tribunals;
- law enforcement;
- tax authorities;

- sanctions enforcement bodies;
- other competent authorities.

7.4 Professional advisers and business counterparties

We may disclose information to auditors, legal counsel, compliance advisers, insurers, acquirers, investors, or transaction counterparties where reasonably necessary and permitted by law.

8. CROSS-BORDER TRANSFERS

We may process or transfer personal information outside the province or country where you are located, including where service providers, banking partners, card partners, affiliates, or infrastructure providers operate in other jurisdictions.

Where personal information of individuals located outside Canada is processed, such information may be transferred to and processed in Canada and other jurisdictions in accordance with applicable laws.

Where personal information originating from the EEA or the United Kingdom is transferred outside those jurisdictions, we will implement such safeguards as may be required under applicable law for the relevant processing activity.

As a result, personal information may be accessible to courts, regulators, law enforcement, or national security authorities in those jurisdictions in accordance with local law.

We take reasonable steps to ensure that personal information transferred to third parties or other jurisdictions remains protected by appropriate contractual, organisational, and security measures.

9. HOW WE PROTECT PERSONAL INFORMATION

We use reasonable administrative, technical, physical, and organisational safeguards designed to protect personal information against loss, theft, unauthorised access, disclosure, copying, misuse, modification, or destruction.

These safeguards may include:

- role-based access controls;
- encryption in transit and, where appropriate, at rest;
- logging and monitoring;
- authentication controls;
- vendor oversight;
- employee confidentiality obligations;
- security testing and incident response processes.

No system is fully secure, and we cannot guarantee absolute security. You also play an important role in protecting your own credentials, devices, and communications.

10. BREACHES OF SECURITY SAFEGUARDS

Where required by law, we will assess breaches of our security safeguards and notify affected individuals, regulators, or other parties where the legal threshold for reporting or notification is met.

PIPEDA includes breach-reporting and notification obligations where a breach creates a real risk of significant harm.

11. RETENTION OF PERSONAL INFORMATION

We retain personal information only for as long as necessary for the fulfilment of the identified purposes, the management of the client relationship, compliance with legal or regulatory obligations, dispute handling, enforcement, and recordkeeping. AML/ATF and transaction records are retained for a minimum of five (5) years from the date the record was created or the business relationship ended, unless longer retention is required by law or applicable holds.

Retention periods may vary depending on:

- the type of service;
- the nature of the information;
- applicable AML / ATF and financial-services obligations;
- limitation periods;
- litigation or investigation holds;
- tax and accounting rules.

When personal information is no longer required, we will delete, destroy, anonymise, or de-identify it where appropriate, subject to legal and operational requirements.

12. ACCESS, CORRECTION, AND COMPLAINTS

Subject to applicable law, including PIPEDA and, where applicable, GDPR or UK GDPR, you may request:

- access to personal information we hold about you;
- correction of inaccurate or incomplete personal information;
- information about how we have used or disclosed your personal information.

We may require verification of identity before responding to such requests. We may also limit access where permitted or required by law, including where disclosure would reveal personal information about another person, confidential commercial information, or legally restricted information.

13. CHILDREN'S PRIVACY

Our services are not intended for minors. We do not knowingly provide services directly to children or knowingly collect personal information from children in connection with our regulated financial services.

14. MARKETING COMMUNICATIONS

Where permitted by law, we may send you service-related, business, or marketing communications. You may opt out of marketing communications using the unsubscribe mechanism provided or by contacting us, although we may still send non-marketing messages relating to your account, transactions, compliance, or legal obligations.

15. COOKIES AND SIMILAR TECHNOLOGIES

We may use cookies, pixels, log files, and similar technologies to:

- operate and secure the website and platform;
- remember preferences;
- analyse performance and usage;
- improve user experience;
- support communications and, where permitted, marketing.

Further details may be set out in our Cookie Policy or cookie notice.

16. CHANGES TO THIS PRIVACY POLICY

We may amend, supplement, restate, or replace this Privacy Policy from time to time.

The updated version will be posted on our Website or otherwise made available to you. Changes will take effect on the date stated in the revised policy.

17. CONTACT US

If you have questions, complaints, or requests relating to this Privacy Policy or our handling of personal information, please contact us using the contact details published on our Website.

General privacy and support contact: **privacy@cepheus-pay.com**

If you are not satisfied with our response, you may have the right to complain to the **Office of the Privacy Commissioner of Canada** or another applicable privacy regulator, depending on the circumstances. PIPEDA provides a complaint framework through the OPC.