CROHOPAY GLOBAL CORP. — Privacy Policy
Version 1.0 · Effective date: 11 November 2026 · Last updated: 11 November 2026

This Privacy Policy explains how CROHOPAY GLOBAL CORP. ("we", "us", "our") collects, uses, discloses and protects personal information. It applies to our clients and people who apply to become clients, visitors to our website, people who contact us and job applicants.

1. Who is responsible
1.1 CROHOPAY GLOBAL CORP., 422 Richards St, Unit 170, Vancouver, BC V6B 2Z4, is responsible for the personal information we hold. We comply with the Personal Information Protection Act (British Columbia) and, where it applies, the Personal Information Protection and Electronic Documents Act (PIPEDA).
1.2 Our Privacy Officer is accountable for our compliance with this Policy. You can contact the Privacy Officer at support@crohopay.ca with the subject "Privacy request".

2. What we collect
Depending on how you deal with us, we collect:
(a) identity and contact information: name, date of birth, residential address, email address, phone number, citizenship, country of birth and country of residence;
(b) identity documents: images of your government-issued photo ID;
(c) biometric information: the selfie video and the results of the comparison with your ID (see section 6);
(d) information we must ask for by law: occupation, source of funds and wealth, purpose of your purchase, whether you act for someone else, and whether you are a politically exposed person or head of an international organization, or related to one;
(e) declarations you give at registration and in your Order Summary & Client Declaration, including whether you are a US person;
(f) payment information: the name, bank and account details of the account you pay from, including the name of any other holder of a joint account, and payment references;
(g) wallet and blockchain information: your wallet addresses, proof that you control them and the transactions linked to them;
(h) order information: amounts, rates, fees, dates, statuses and transaction hashes;
(i) technical information: IP address, device and browser information, location signals and information about your use of our website and client area;
(j) communications: your emails, messages through our contact form, recordings and notes of phone calls, complaints and reports;
(k) for job applicants: your CV and the information in your application.

3. How we collect it
3.1 Most information comes directly from you, when you register, verify your identity, submit an order request, pay, sign documents or contact us. If you give us information about another person, such as the other holder of a joint account, please make sure they are aware of this Policy.
3.2 Some information is collected automatically when you use our website and client area, including through cookies (see our Cookie Policy).
3.3 We also receive information from our identity verification provider, from sanctions,

politically exposed person and adverse media databases, from blockchain analytics providers, from banks and payment providers, and from public sources.

4. Why we use it

We use personal information to:
(a) open and manage your account and provide our service;
(b) verify your identity and meet our obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and sanctions laws, including screening, monitoring, record keeping and reporting;
(c) check your payments and wallets, process orders and refunds;
(d) prevent fraud and scams, protect your account and keep our systems secure, including applying location restrictions;
(e) communicate with you about your account, orders and changes to our documents, and handle your requests and complaints;
(f) consider job applications;
(g) meet our accounting, tax and other legal obligations and protect our legal rights.
We do not send promotional emails and we do not sell personal information.

5. Consent

5.1 We collect, use and disclose personal information with your consent, except where the law allows or requires otherwise. By registering and using our service, you consent to the uses described in this Policy.
5.2 Some information is required by law. If you do not provide it, we cannot open an account for you or provide our service.
5.3 You may withdraw your consent at any time, subject to legal and contractual limits. If you do, we may not be able to continue providing our service. We will keep the information the law requires us to keep.

6. Biometric information

6.1 With your express consent, our identity verification provider compares a short selfie video with the photo on your ID to confirm that you are the holder of the document and that you are present.
6.2 We use biometric information only for identity verification, fraud prevention and our legal obligations. We do not use it for any other purpose and do not sell or share it for marketing.
6.3 We keep it as part of our identification records for as long as the law requires.
6.4 If you do not consent to biometric verification, we cannot complete your identity verification and cannot provide our service.

7. Automated checks

Identity verification and screening are partly automated. If an automated check leads to a decision you disagree with, you can ask for a member of our team to review it.

8. Who we share it with

8.1 We share personal information only as needed with:
(a) service providers that help us provide our service, including our identity verification and screening provider, blockchain analytics provider, client area and order management provider,

electronic signature provider, telephone service provider, website hosting provider and email and document storage provider;
(b) banks and payment service providers that process your payments and refunds;
(c) our accountants, lawyers, auditors and the independent reviewer of our compliance program;
(d) FINTRAC, law enforcement and other government authorities, where the law requires or allows;
(e) a buyer or successor of our business, under confidentiality obligations; and
(f) anyone else with your consent.
8.2 Our service providers may use personal information only to provide services to us and must protect it under written agreements.
8.3 The law may prohibit us from telling you that we have disclosed information to FINTRAC or another authority.

9. Storage outside Canada
Personal information may be stored or processed outside Canada, including in the European Union, the United Kingdom and the United States, by our service providers. While it is outside Canada, it may be accessed by the courts, law enforcement and national security authorities of those countries under their laws. We remain responsible for it and protect it through written agreements and security measures.

10. How long we keep it
10.1 We keep client records for at least five years after the date they are created or after your account is closed, as the PCMLTFA requires, even if you ask us to delete them.
10.2 We keep job applications for 12 months after the role is filled, unless you ask us to delete yours earlier.
10.3 We keep other personal information only as long as we need it for the purposes in this Policy or as the law requires. Then we delete it or make it anonymous.
10.4 We keep recordings of phone calls for 12 months. Where a call concerns a complaint or a matter we must review under our legal obligations, we keep the recording with your client records.

11. How we protect it
We protect personal information with security measures appropriate to its sensitivity, including access limited to staff who need it, multi-factor authentication, encryption and written agreements with our service providers. No method of transmission or storage is completely secure.

12. Privacy breaches
If a breach of security safeguards involving your personal information creates a real risk of significant harm to you, we will notify you and the Office of the Privacy Commissioner of Canada or the Office of the Information and Privacy Commissioner for British Columbia, as the law requires, and we keep a record of every breach.

13. Your rights
13.1 You can ask to access the personal information we hold about you and to correct it if it is inaccurate or incomplete. We respond within 30 days and do not charge a fee.

13.2 We will verify your identity before we respond.
13.3 In some cases the law allows or requires us to refuse access, for example where the information concerns a report to FINTRAC, would reveal personal information about someone else or is subject to legal privilege. If we refuse, we tell you why, unless the law prohibits it.
13.4 If you are not satisfied with how we handle your personal information, please contact our Privacy Officer first. You can also complain to the Office of the Information and Privacy Commissioner for British Columbia or the Office of the Privacy Commissioner of Canada.

14. Phone calls and messages
We record phone calls to keep an accurate record of requests and instructions, to handle complaints and to prevent fraud. We tell you at the start of each call that it is recorded. Recordings are kept as set out in section 10.

15. Cookies
Our use of cookies and similar technologies is explained in our Cookie Policy.

16. Minors
Our service is only for people who have reached the age of majority in their province or country of residence. We do not knowingly collect personal information from minors.

17. If you are in the European Union or the European Economic Area
We are established in Canada and do not target persons in the EU/EEA. We process personal information under Canadian law. The European Commission has recognized Canada as providing an adequate level of protection for personal information handled by organizations subject to PIPEDA.

18. Changes
We may change this Privacy Policy by publishing a new version, with its effective date, on our website. If a change materially affects how we use your personal information, we will tell you by email before it takes effect.

19. Contact
Privacy Officer, CROHOPAY GLOBAL CORP., 422 Richards St, Unit 170, Vancouver, BC V6B 2Z4 · support@crohopay.ca (subject "Privacy request")