Clarity Global Inc

Privacy Policy

2026

Clarity Global

Clarity Global Inc. — 2026

PRIVACY POLICY

1. About this policy

We aim to be transparent. We care about our business, and you are key to it, so we do not hide behind complex wording and fine print. This Privacy Policy explains what personal information Clarity Global Inc. ("Clarity", "we", "us") collects, why, how we use and share it, and the choices and rights you have.

We handle personal information in accordance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and Alberta's Personal Information Protection Act (PIPA). Where other laws apply to you, such as UK or EU data protection law, we also comply with them.

As a money services business registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), we are also subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), Canadian sanctions laws, and the Retail Payment Activities Act, under which we are registered with the Bank of Canada. These laws require us to collect, verify, keep and report certain information about our clients and their transactions. Where they conflict with a choice or right described in this policy, we must follow the law, and this policy explains where that happens.

"Personal information" means information about an identifiable individual. It does not include aggregated or de-identified data that cannot reasonably be used to identify you.

2. Who we are and who is accountable

Clarity Global Inc. is responsible for personal information under its control. We have designated a Privacy Officer who is accountable for our compliance with this policy and applicable privacy law.

Company legal name	Clarity Global Inc.
Address	22-1100 8 Ave SW, Calgary, Alberta, T2P3T8, Canada
FINTRAC MSB registration number	M22927420
Privacy Officer	Oleksii Ivashchenko, MLRO/ CCO
Privacy contact	[privacy@clarityglobalinc.com] (currently info@clarityglobalinc.com)

You can contact the Privacy Officer with any question about this policy, to exercise your rights, or to obtain written information about our use of service providers outside Canada.

3. Who this policy covers

Clarity is the organization accountable for the personal information described here. This policy applies to:

Individual clients who use our services.
Business clients and the people connected to them: directors, officers, beneficial owners, authorized signatories and employees who act for the business, etc.
Recipients and senders of funds involving our clients, whose details we receive to complete a transaction.
Applicants and prospects who start sign-up or contact us about our services.
Website and app visitors.

When you give us information about another person, such as a recipient, a beneficial owner or a co-signatory, you confirm that you are allowed to share it and that you have told them about this policy.

4. Personal information we collect

We collect what we need to provide our services and what the law requires us to collect.

Category	Examples
Identity and contact	Full name, home or business address, date of birth, occupation or nature of business, telephone number, email
Identity verification	Type, number, issuing jurisdiction and expiry date of government-issued photo ID; information from your credit file or other reliable sources used to confirm identity; a facial image and liveness data
Business client information	Legal name, address, incorporation and registration records, nature of business, directors, beneficial owners and the ownership and control structure, authorized signatories
Compliance information	Whether you are a politically exposed person, head of an international organization, or their family member or close associate; whether you act for a third party; source of funds or wealth; purpose of the business relationship; sanctions and adverse media screening results; our risk assessment
Transaction and account	Account details, transaction amounts, dates and currencies, sender and recipient names, addresses and account numbers, bank account and payment instrument details
Communications	Messages, support requests, complaints and your marketing preferences

Category	Examples
Technical and device	IP address, device identifiers, approximate location derived from IP, browser type, login and activity records, used for security and fraud prevention
Aggregated data	Statistics that do not identify you, such as transaction volumes by corridor

Much of this information is sensitive, and we protect it accordingly. We collect identity, compliance and transaction information because the PCMLTFA and sanctions laws require it; we cannot provide our services without it.

Biometrics. If you verify your identity with a selfie, we compare it with the photo on your ID. We do this only with your consent and use the data only for identity verification. We keep it with your other identity verification records for at least 5 years. You can choose to verify your identity another way instead.

Aggregated data is derived from personal information but does not identify you. If we combine it with personal information so that it could identify you, we treat the result as personal information.

5. How we collect it

- Directly from you, when you apply, open an account, verify your identity, send or receive funds, contact us, or respond to our requests for information.
- From identity verification and screening providers, sanctions, politically exposed person and adverse media databases, and public corporate registries.
- From banks, payment networks and other financial institutions, including information about the sender or recipient that travels with a transfer.
- From business clients, about their directors, beneficial owners, signatories and employees.
- Automatically, through cookies, device and login data when you use our website and app (see section 7).

6. Why we use it and on what basis

We identify our purposes at or before collection and use your information only for them, unless you consent to a new purpose or the law permits or requires otherwise.

Purpose	Basis
Opening and managing your account, processing transfers and exchanges, customer support	Your consent and our agreement with you
Verifying identity, screening against sanctions and politically exposed person lists, assessing risk, monitoring transactions	Required by the PCMLTFA and Canadian sanctions laws

Purpose	Basis
Reporting to FINTRAC and responding to lawful requests from authorities	Required by law
Detecting and preventing fraud, and securing our systems	Permitted by law and your consent
Record-keeping, tax, accounting and audit	Required by law
Improving our services and website	Your consent (implied for non-sensitive usage data)
Marketing	Your consent, as required by CASL

Information the law requires. You cannot withdraw consent to the collection, use or disclosure the law requires. If you do not provide it, we cannot open an account or process a transaction, and we may have to end our relationship with you.

Reports made without notice. We must report certain transactions to FINTRAC, including suspicious transactions of any amount and large cash, electronic funds and virtual currency transactions of $10,000 or more. The law prohibits us from telling you whether we have made a suspicious transaction report.

Other consent. For everything else, we rely on your consent, express or implied depending on the sensitivity of the information and your reasonable expectations. You may withdraw it at any time by contacting our Privacy Officer, subject to legal or contractual limits. We will explain the consequences, such as being unable to continue a service. Withdrawal does not affect use that took place before it.

Automated decisions. We use automated tools to verify identity, screen against sanctions lists and detect fraud. Our compliance staff review flagged results before any decision is made, so no decision about you is made solely by automated means. If that changes, we will tell you, explain the main factors on request, and let you ask a person to review it.

7. Cookies and tracking technologies

Our website and app use cookies and similar technologies. Essential cookies make them work and keep your account secure. Analytics cookies, set through Google Analytics and Google Tag Manager, help us understand how visitors use our public website. We do not run analytics or advertising tags on logged-in account, verification or transaction pages.

You can accept or decline non-essential cookies through our cookie banner and change your choice at any time through [Cookie settings link]. You can also block cookies in your browser or install the Google Analytics opt-out browser add-on (tools.google.com/dlpage/gaoptout).

8. Marketing emails

We send commercial electronic messages only in line with Canada's Anti-Spam Legislation (CASL): with your express consent, or where CASL allows implied consent, such as an existing business relationship or a business address you have published without saying you do not want messages. Every message identifies Clarity, includes our contact details, and has a working unsubscribe link. We act on unsubscribe requests within 10 business days.

Service messages, such as transaction confirmations, security alerts and requests for information we are required to collect, are not marketing. You will receive them while you have an account with us.

9. Sharing and processing outside Canada

We do not sell your personal information. We share it only as follows:

- Regulators and authorities. With FINTRAC for required reports; with the Canada Revenue Agency, law enforcement and other authorities where the law requires or permits, such as under a production order or warrant; and with the Bank of Canada under the Retail Payment Activities Act.
- Banks, payment networks and receiving institutions. To complete your transactions. As the law requires, sender and recipient details travel with each transfer to the institutions that handle it, including abroad.
- Service providers that perform services for us (table below). Our contracts limit them to that purpose and require protection comparable to ours.
- People you authorize, such as a representative or, for business clients, their authorized signatories.
- A buyer or successor in a business transaction, under an agreement to protect the information.

Service provider	Purpose	Location	Protection
SumSub	Identity verification and biometric matching	[Country]	Encryption in transit and at rest
SumSub	Sanctions, politically exposed person and adverse media screening	[Country]	Encryption in transit and at rest
Banking and payment partners	Processing transactions	UK and EU	Encryption in transit and at rest
[Cloud hosting provider]	Hosting our platform and records	[Country]	[Encryption in transit and at rest]

Service provider	Purpose	Location	Protection
Freshsales	Customer relationship management	United States	Encryption in transit and at rest
Google Analytics and Google Tag Manager	Public website analytics	United States	Encryption in transit and at rest

Processing outside Canada. Some of our service providers store or process personal information outside Canada, and international transfers send information to institutions in the destination country. While outside Canada, your information is subject to local laws and may be accessed by courts, law enforcement and national security authorities there. You can obtain written information about our policies and practices for service providers outside Canada, or ask questions about their handling of your information, by contacting our Privacy Officer.

UK and EEA individuals. When we transfer personal information of UK or EEA individuals, we rely on an adequacy decision (Canada holds one from the European Commission for commercial organizations) or on approved standard contractual clauses.

10. How we protect it

We protect personal information with safeguards appropriate to its sensitivity. Identity, compliance and transaction data are encrypted in transit and at rest. Access is limited to staff who need it for their role, such as our compliance team, and is logged. Staff are bound by confidentiality, trained on privacy and anti-money-laundering obligations, [and background-checked]. We use multi-factor authentication for client accounts and internal systems.

Breaches. If a breach of security safeguards creates a real risk of significant harm to you, we will notify you and report it to the Office of the Privacy Commissioner of Canada or the Office of the Information and Privacy Commissioner of Alberta, as applicable, as soon as feasible. We will also report incidents to the Bank of Canada, and notify affected clients, as the Retail Payment Activities Act requires. We keep a record of every breach for at least 5 years.

Where you have a password for our applications, please keep it confidential and do not share it.

11. How long we keep it

We keep personal information as long as needed for the purposes it was collected for and as long as the law requires. When we no longer need it, we securely destroy it or make it anonymous.

Information	Retention period
Identity verification (including biometric data), beneficial ownership and other client records	At least 5 years after the account closes or the business relationship ends

Information	Retention period
Transaction records and reports made to FINTRAC	At least 5 years from the date the record was created
Billing, tax and accounting records	At least 6 years after the end of the tax year, as required by the Income Tax Act
Applicant records where no account was opened	At least 5 years
Prospect and marketing records	At least 5 years after last contact
Website analytics data	14 months, the maximum our analytics provider retains
Breach records	At least 5 years

These legal periods apply even if you close your account or ask us to delete your information. We may keep information longer in the event of a complaint, investigation or reasonably anticipated litigation.

12. Your rights

You have the right to:

- Access the personal information we hold about you, learn how it has been used, and to whom it has been disclosed, subject to the limits below.
- Correct information that is inaccurate or incomplete. For verified identity details, we may ask for supporting documents. Where appropriate, we will send the correction to third parties that received the information.
- Withdraw consent where we rely on it, as described in section 6.
- Challenge our compliance with this policy by contacting our Privacy Officer, and complain to a regulator (see section 13).

If UK or EU law applies to you, you also have the rights it gives you, including erasure, restriction, objection and portability.

Limits that apply to a financial services business. We cannot delete or stop using information we must keep under the PCMLTFA or other laws until the required retention period ends, even if you ask, including under UK or EU law. If your request concerns information we have disclosed to FINTRAC or another government institution, the law requires us to consult that institution first and may require us to refuse. In that case we will notify the Privacy Commissioner of Canada, and we may not be able to tell you about the disclosure.

How to make a request. Send a written request to our Privacy Officer. We may ask for information to verify your identity, and we use it only for that purpose. We will respond within 30 days (45 days for requests under Alberta's PIPA). If we need more time, we will tell you within that period, why, and when to expect our answer. Requests are free, unless they are clearly unfounded or excessive, in which case we will tell you the minimal cost in advance. If we refuse a request, we will explain why in writing and tell you how to challenge the decision. In some cases, such as where information would reveal another person's information or is subject to legal privilege, the law allows or requires us to withhold it.

13. Questions and complaints

Please contact our Privacy Officer first; we investigate every complaint and, if it is justified, take appropriate measures, including changing our practices. You may also complain to a regulator at any time:

Regulator	Who it covers	Website
Office of the Privacy Commissioner of Canada	Most individuals in Canada	www.priv.gc.ca
Office of the Information and Privacy Commissioner of Alberta	Information collected, used or disclosed in Alberta	www.oipc.ab.ca
Your local data protection authority	UK and EEA residents	Varies

14. Other matters

Eligibility and minors. Our services are available only to individuals who have reached the age of majority in their province or territory of residence, and to legally registered businesses. We do not offer our services to residents of Quebec or to businesses located there. Our website and app are not directed at children, and we do not knowingly collect personal information from minors. If you believe we have, please contact us and we will delete it unless the law requires us to keep it.

Third-party links. Our website may link to third-party websites, plug-ins and applications. Clicking those links or enabling those connections may allow third parties to collect or share data about you. We do not control them and are not responsible for their privacy practices, so please read their privacy policies.

Changes to this policy. We may update this policy from time to time. We will post the new version with its effective date on this page and, for significant changes, notify you by email or a notice on our website before they take effect. If a change involves a new purpose that requires your consent, we will ask for it.