

Privacy Policy

Siimply Trade Inc. (17196172 Canada Inc.)

Last updated: August 2026

Protecting your privacy and the security of your personal data is critically important to SiimplyTrade. This Privacy Policy explains what information we collect about you, how we use and share that information, and your rights in relation to it.

By using SiimplyTrade's services, you agree to the collection, use, disclosure, and procedures described in this Privacy Policy. If you do not agree with these terms, please do not use the platform. We may update this Privacy Policy from time to time as laws or our services change, and we will notify you of any significant updates.

1. Data Controller and Data Protection Officer

For the purposes of data protection law, the platform is operated by Siimply Trade Inc. (17196172 Canada Inc.), a Canadian company, which is the contracting entity and a data controller of your personal information collected in connection with using our platform. Our Zimbabwean operating subsidiary is also a controller for personal information processed in connection with local Zimbabwean services.

InvestIQ, FBC and Alpaca, when handling your data for their respective services such as execution, custody, foreign exchange and KYC, act as independent controllers for those processes. We coordinate with them to ensure consistency and protection of your data across borders.

We have appointed a Data Protection Officer to oversee our data protection compliance. The DPO's contact details are provided in the Contact Us section of this Policy.

2. Information We Collect

We collect several categories of personal information from you, and sometimes from third parties, to provide our services:

- Personal identifiers: full name, date of birth, nationality, and government-issued identification details such as national ID, passport, or driver's licence number, together with copies of those documents as part of KYC. We may also collect a social insurance or tax identification number where needed for tax forms.
- Contact information: phone number, email address, residential address, and mailing address, and any alternative contact or next-of-kin details you provide.
- Financial information: bank account and mobile money details, card information if used for funding, and relevant transaction history. We also collect income range, employment status, occupation, and net worth or investment experience where required by KYC rules.
- Transaction and account information: details of trades you execute, account balances in each wallet, deposits and withdrawals, securities lending activity, and portfolio performance data.
- Compliance information: results of identity verification, risk scores, sanctions or watchlist hits, politically exposed person status, and compliance notes, together with documents you provide such as proof of address or source of funds. Sensitive data such as biometric data used for identity verification is processed under strict conditions, typically with your explicit consent where required by law.

- Technical and usage data: device type, operating system, app version, IP address, device identifiers, log information, and general or precise geolocation where enabled. We use cookies and similar technologies on our website.
- Communications: copies of your communications with us by email, chat, in-app messaging, or phone. Support calls may be recorded for quality and security.
- Preferences and feedback: communication preferences, language choice, feature opt-ins, and any feedback or survey responses.
- Publicly available or third-party data: information from credit bureaus or identity databases, referral programmes, public registries, and from InvestIQ, FBC and Alpaca regarding your onboarding status and account information.

We limit collection to what is necessary for the identified purposes. We do not collect religious or political beliefs, health data, or precise biometrics unless absolutely required. Our service is not offered to minors, and if we learn that we hold information about someone under 18 we will delete it and close the account, subject to any legal retention requirement.

3. How We Use Personal Information

Account setup and authentication: we use personal identifiers, contact information, and KYC documents to verify your identity at signup, set up your accounts, and authenticate you at login or when performing sensitive actions.

Service delivery: to provide the trading and investment services you request, including executing and confirming trades, maintaining your wallets, processing deposits and withdrawals, administering any separately enrolled securities lending service where offered, issuing statements, confirmations and portfolio summaries, and communicating with you about your account.

Compliance and risk management:

- Anti-money-laundering: screening and monitoring using identification, background, and transaction data, including checks against sanctions lists maintained by Zimbabwe's Financial Intelligence Unit, OFAC, and other global watchlists.
- KYC and due diligence: determining eligibility using nationality, financial background, and any politically exposed person status.
- Fraud prevention: using device and usage data to detect unusual access, account takeover attempts, or scam behaviour, with human oversight where required by law.
- Regulatory reporting: preparing reports required by regulators, including SECZim, Alpaca's reporting to applicable tax authorities, and Canadian or other authorities under information-sharing agreements such as CRS.
- Secure operations: enforcing our terms and policies, investigating suspected prohibited use, and maintaining platform security.

Service improvement and analytics: we analyse usage data, feedback, and aggregate transaction data to improve our platform, using anonymised or aggregated data where possible.

Personalisation: we may use your data to personalise your experience, such as remembering preferences or customising educational content relevant to your portfolio.

Marketing and communication: we may send promotional communications about new features, products, or offers in compliance with applicable laws including CASL and CAN-SPAM. You can opt out at any time. We do not sell your data to third-party marketers.

Cross-border service delivery: because we are a cross-border platform, your data may be used in one country to facilitate action in another, for example using Zimbabwe KYC data to help Alpaca satisfy US onboarding requirements.

Legal defence and rights: we may use and preserve relevant personal information as evidence and to protect our legal rights, including sharing with our legal advisers and courts or arbitrators as needed.

We will seek your consent before using your personal data for any purpose that is not compatible with the original purposes for which it was collected, unless otherwise required or permitted by law.

4. Legal Bases for Processing

In Zimbabwe, processing is allowed with consent or for legitimate purposes under the applicable Act. Under PIPEDA in Canada, organisations must have consent, implied or explicit depending on sensitivity, except where exemptions apply. In the US, financial companies rely on consumer consent or their privacy notices, with opt-out for certain sharing.

We primarily rely on consent, contractual necessity, legal obligation, and legitimate interests such as improving our service or preventing fraud, balanced against your privacy rights. When we process sensitive data such as biometrics, we do so under explicit consent or strict necessity for compliance.

5. How We Share Personal Information

Core service partners: we share data with InvestIQ, FBC and Alpaca to carry out the services, including forwarding KYC details and documents for account opening and sharing relevant transaction data. As independent controllers, they have their own obligations to protect your data and are contractually bound to maintain confidentiality and security.

Within the Siimplify group: our corporate structure includes Siimplify Trade Inc. in Canada and its Zimbabwean subsidiary, and may include other affiliates in the future. We share data within the group on a need-to-know basis under strict confidentiality and the same security standards.

Service providers: we use processors such as cloud hosting providers, identity verification services, payment processors and banking partners, communication tools, analytics tools, and customer support tools. They may not use your data for their own purposes and we execute data processing agreements where required.

Regulators and authorities: we may disclose personal information to regulators, law enforcement, or government agencies where required by law, including SECZim, RBZ, ZIDA or the FIU in Zimbabwe, US authorities via Alpaca, and Canadian authorities where applicable. We verify the legitimacy of requests and narrow disclosure to what is legally required.

Business transfers: if Siimplify Trade Inc. or an affiliate goes through a merger, acquisition, restructuring, or asset sale, your personal data may be transferred as part of that transaction. We would ensure the new entity continues to protect your data under this policy and notify users of a change of controller.

Affiliates and partners: aside from InvestIQ, FBC and Alpaca, any other sharing with third parties for their own use would only be done with your knowledge and consent.

Aggregate or anonymised data: we may share information in aggregate form such that no individual is identifiable, taking care to prevent re-identification.

We do not sell or rent your personal information to third-party companies for their independent marketing purposes, and we do not share account or transactional data with any third party for them to advertise to you.

Retention by recipients: recipients such as Alpaca, FBC and InvestIQ have their own retention obligations under AML and securities laws. Even if you ask us to delete your data, we cannot compel those partners to delete records they are legally required to keep.

6. International Data Transfers and Safeguards

SiimplyTrade is a cross-border service, so your data is transferred and processed in multiple countries, including Zimbabwe where our local operations are conducted and where InvestIQ and FBC operate, Canada where Siimply Trade Inc. is located, and the United States and other jurisdictions where Alpaca and some of our infrastructure may be located.

Whenever we transfer personal data out of its country of origin, we ensure adequate safeguards are in place:

- Transfers from Zimbabwe: Zimbabwe's Data Protection Act requires licensing and safeguards by data controllers. Where we send data to a processor in another country, we put in place a contract protecting that data to comparable standards.
- Transfers from Canada: PIPEDA holds us accountable for ensuring comparable protection by the foreign recipient. We sign contracts with confidentiality and data protection clauses, inform users that their information may be processed abroad, and transfer only what is necessary using secure methods.
- Encryption and security: regardless of location, we employ strong encryption for data in transit and at rest, access controls, and multi-factor authentication for systems containing personal data.

By using SiimplyTrade, you agree that we may transfer your data internationally as needed to provide the service. Different countries have different laws, and data held in another jurisdiction may be subject to access by that jurisdiction's authorities. We mitigate undue access by sharing only what is necessary and pushing back legally where appropriate.

7. Data Security Measures

SiimplyTrade employs a variety of measures to guard your personal and financial information against loss, theft, misuse, and unauthorised access or disclosure:

- Encryption: network communications involving personal data are encrypted using industry-standard protocols such as TLS 1.2/1.3, and sensitive data is encrypted at rest.
- Access controls: employee and contractor access is granted on a need-to-know basis with role-based access control, multi-factor authentication, strong password policies, and audit logs.
- Physical security: physical records are kept in secure facilities and cloud data is stored in secure data centres with surveillance and controlled entry.
- Security testing and audits: regular internal code reviews, periodic penetration testing by independent experts, and vulnerability scanning.
- Organisational measures: personnel training on data protection, confidentiality agreements, and background checks for sensitive positions where permitted by law.
- Data minimisation and pseudonymisation: masking or using dummy data in development and testing environments where feasible.
- Third-party security: we vet service providers for strong security practices and appropriate certifications such as PCI-DSS, ISO 27001, or SOC 2.

- Account security for users: features such as two-factor authentication and activity alerts. We will never contact you unsolicited to ask for your password or full 2FA code.
- Monitoring: intrusion detection, log monitoring, and alerting for unusual activity or unauthorised access attempts.

Despite these measures, no system is completely secure and we cannot guarantee absolute security. In the event of a data breach affecting your personal information, we have procedures to notify affected individuals and regulators as required.

8. Data Retention and Disposal

We retain your personal information only for as long as necessary to fulfil the purposes for which it was collected, or as required or permitted by law.

Regulatory retention: financial and KYC data must often be kept for a minimum period. Zimbabwean regulations and international AML standards typically require retaining customer identification and transaction records for at least five years after the end of the customer relationship. US brokerage records held by Alpaca may need to be kept for a number of years under applicable law.

Operational retention: we keep data for as long as your account is active. If your account becomes inactive we may archive rather than delete it, because dormant accounts may be reactivated or must be maintained for audit.

Disputes and investigations: if you or we are involved in a dispute, investigation, or litigation, we will retain relevant information until it is resolved.

Examples of retention periods:

- Contact and account information: the life of the account plus five years after closure.
- Transaction records: at least seven years.
- Communications such as support chats and emails: two to three years after resolution, unless needed longer.
- Device and usage logs: typically one to two years, unless flagged for security review.
- Biometric or verification data: typically deleted or archived once verification is complete, retaining evidence of verification; ID documents are kept as part of the KYC record for five years or more.
- Incomplete registrations: partial records may be purged after a shorter period, such as six months, unless law requires otherwise.

Legal hold: if we receive a litigation hold or similar instruction, or we are aware of potential litigation, we will suspend deletion of the relevant data until cleared.

After the retention period we securely delete personal information or irreversibly anonymise it. Where you request deletion, we will delete data that we are not legally required to retain and explain what we cannot delete and why.

9. Your Rights and Choices

Subject to applicable law, you have the following rights regarding your personal information:

- Right to access: request a copy of the personal data we hold about you and information on how we use it, typically within 30 days or the timeframe required by law.
- Right to rectification: ask us to correct inaccurate or incomplete information.

- Right to withdraw consent: withdraw consent at any time where we rely on it, without affecting the legality of prior processing.
- Right to object: object to processing for particular purposes, including direct marketing, which we will always honour.
- Right to erasure: request deletion of your personal data in certain circumstances, subject to records we must retain by law such as KYC records.
- Right to data portability: request a copy of data you provided in a machine-readable format where the applicable regime provides this right.
- Right to challenge automated decisions: request human review of automated decisions that have a legal or significant effect on you.
- Right to complain: lodge a complaint with the relevant data protection authority, being the Data Protection Authority under POTRAZ in Zimbabwe, the Office of the Privacy Commissioner in Canada, or the FTC or relevant securities regulator in the US. We encourage you to contact us first.
- Right to opt out of marketing: unsubscribe from marketing emails or texts at any time. Transactional and service messages are part of the service and are not optional.
- Rights relating to cookies: set your browser to refuse cookies, and use our website cookie banner to opt out of non-essential cookies.
- Non-discrimination: we will not deny you services or provide lesser service because you exercise a privacy right, although certain deletions or restrictions may mean we cannot continue to provide full service.

10. Exercising Your Rights

To exercise any of your rights, contact us at the address below or through in-app support. We may ask you to verify your identity.

We will respond within the timeframe required by law and aim for 30 days under PIPEDA and Zimbabwean law. If we need an extension, we will inform you and explain why. If we cannot fulfil your request, we will provide an explanation.

We do not typically charge a fee for these requests. Where a request is manifestly unfounded or excessive, some laws allow a reasonable fee or refusal, but we prefer to work with you to refine the request.

11. Privacy of Children

Our services are not intended for individuals under the age of 18, or the age of majority in your jurisdiction. We do not knowingly solicit or collect personal data from minors, and we ask for date of birth as part of account opening to ensure all users are adults.

If we become aware that we have inadvertently collected personal information from someone under 18, we will delete it as soon as possible unless we are legally obliged to retain it, in which case we will secure it and isolate it from further use. Parents or guardians who believe we hold data about their child without proper consent should contact us.

12. Updates to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors. When we make changes, we will post the updated policy on our website and app and adjust the effective date. Where changes are material, we will notify you in advance by email, a prominent notice on our website or in-app, or a prompt at login. Continuing to use our platform after the updated policy becomes effective will be deemed acceptance of the changes, to the extent permitted by law.

13. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data handling practices, please contact us by email at support@siimply.co, marked for the attention of the Data Protection Officer or Privacy Team.

Contracting entity: Siimply Trade Inc. (17196172 Canada Inc.), Canada. Local operations in Zimbabwe are delivered through our Zimbabwean subsidiary.

Your privacy is important to us, and we commit to working with you to ensure that your personal information is handled securely and in accordance with your rights.