Privacy Policy

How NOVARC collects, uses, discloses and protects personal information

EFFECTIVE DATE	16 July 2026
VERSION	1.0
COMPANY	**NOVARC FINANCIAL LTD.**
INCORPORATION NO.	**BC1579964**
REGISTERED OFFICE	C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada
WEBSITE	https://novarc.global/canada

Privacy questions: privacy@novarc.global

1. Who We Are

NOVARC FINANCIAL LTD. is a company incorporated under the laws of British Columbia, Canada, under incorporation number BC1579964, with its registered office at C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada. In this Policy, "NOVARC", "we", "us" and "our" refer to NOVARC FINANCIAL LTD.

NOVARC provides or arranges non-custodial digital asset liquidity, over-the-counter transaction services, fiat-to-crypto, crypto-to-fiat, settlement coordination and related technology and compliance services, subject to eligibility, regulatory requirements and the availability of third-party providers.

NOVARC is accountable for Personal Information under its control, including information processed on its behalf by Service Providers. NOVARC has designated a Privacy Officer to oversee compliance with this Policy and applicable privacy law.

2. Scope and Applicable Privacy Laws

This Policy applies to Personal Information collected, used or disclosed in connection with the NOVARC website, portals, applications, APIs, onboarding and verification processes, customer support, transaction execution, compliance monitoring, business relationships and communications (collectively, the "Platform" and the "Services").

The Policy applies to individuals who use or apply to use the Services and to individuals connected with an organizational customer, including directors, officers, employees, authorized representatives, beneficial owners, shareholders, partners, trustees, counterparties, originators and beneficiaries.

NOVARC handles Personal Information in accordance with applicable Canadian privacy laws, including the British Columbia Personal Information Protection Act ("BC PIPA") and the federal Personal Information Protection and Electronic Documents Act ("PIPEDA") where it applies, including to interprovincial or international commercial activities. Other Canadian provincial privacy requirements may apply depending on the circumstances.

This Policy does not apply to information that is not Personal Information under applicable law, including anonymized or aggregated information that cannot reasonably identify an individual. Certain business contact information may be excluded from the statutory definition of Personal Information, but NOVARC may nevertheless handle it in accordance with this Policy.

Where the law of another jurisdiction applies to a specific individual or processing activity, NOVARC may provide a supplemental notice or apply additional rights and safeguards.

3. Key Definitions

Personal Information: information about an identifiable individual, whether it identifies the individual directly or can reasonably be linked to them.

Customer: an individual or organization that accesses, applies for or uses the Services. For an organizational Customer, relevant individuals include its representatives, directors, officers, owners and counterparties.

Sensitive Information: information that may create a higher risk of harm if misused, including government identification, authentication data, financial information, source-of-funds or source-of-wealth information, biometric or liveness information where used, and transaction or wallet data that reveals sensitive facts.

Service Provider: a third party that processes information or supports NOVARC's operations, including providers of identity verification, payment, banking, liquidity, custody, blockchain analytics, security, cloud, communications and professional services.

External Wallet: a blockchain address or wallet not controlled or custodied by NOVARC.

4. Privacy at a Glance

What we collect	Identity, corporate ownership, contact, financial, transaction, wallet, blockchain, compliance, communications and device information.
Why we use it	To onboard and verify Customers, provide and secure the Services, execute and settle transactions, comply with AML/ATF and other legal obligations, prevent fraud and manage risk.

Who receives it	Service Providers, financial institutions, transaction counterparties, NOVARC affiliates, professional advisers and competent authorities where necessary or lawful.
Cross-border processing	Information may be processed outside British Columbia or Canada and may be subject to the laws of the receiving jurisdiction.
Your choices and rights	You may request access or correction, withdraw consent where applicable, unsubscribe from marketing and raise a privacy complaint.
Our commitment	We do not sell or rent Personal Information to third parties for their independent marketing purposes.

5. Personal Information We Collect

The categories collected depend on the Services requested, the Customer type, the transaction, applicable law, NOVARC's risk controls and Service Provider requirements. NOVARC may collect the following information:

5.1 Identification and verification information

- full name, former names or aliases, date of birth, nationality, citizenship, residential address and tax residence;
- government-issued identification, document numbers, issuing authority, expiry date and verification results;
- photographs, selfies, liveness checks and facial comparison results, and biometric information where processed by an identity-verification provider and permitted by law;
- occupation, employer, position, tax identification numbers and other information required to verify identity or eligibility.

5.2 Business, authority and beneficial ownership information

- legal and trading names, jurisdiction, incorporation or registration number and registered or principal business address;
- directors, officers, authorized representatives, shareholders, partners, trustees and ultimate beneficial owners;
- ownership and control charts, constitutional records, resolutions, powers of attorney, licences, regulatory status and nature of business;
- information about intended use, expected transaction activity, customers, suppliers, counterparties, geographic exposure and source of funds or wealth.

5.3 Financial, transaction and blockchain information

- bank account, payment and settlement details, account ownership evidence and payment status;
- Quotes, Orders, transaction amounts, currencies, fees, timestamps, instructions, confirmations and settlement records;
- wallet addresses, transaction hashes, blockchain network information, ownership or control evidence and blockchain activity;
- blockchain analytics, wallet risk indicators and exposure to sanctioned, stolen, illicit or high-risk addresses, services or protocols;
- originator, beneficiary and transaction information required under the travel rule or comparable information-sharing requirements.

5.4 Compliance and risk information

- sanctions, politically exposed person, head of international organization and related-person screening results;
- adverse media, fraud, litigation, insolvency, regulatory and law-enforcement information obtained from lawful sources;
- source-of-funds, source-of-wealth, purpose-of-transaction and expected-activity information;
- risk scores, monitoring alerts, case notes, enhanced due diligence records and decisions concerning onboarding or transactions.

5.5 Contact, communications and support information

- email address, telephone number, mailing or business address and communication preferences;
- messages, inquiries, complaints, meeting notes, support interactions and information submitted through forms or questionnaires;
- call recordings or transcripts where calls are recorded after appropriate notice and where permitted by law.

5.6 Technical and usage information

- IP address, device identifiers, browser type, operating system, language, time zone and approximate location;
- login and authentication events, pages viewed, links clicked, timestamps, error logs and security telemetry;
- cookie identifiers and information collected through similar technologies.

6. Sources of Personal Information

NOVARC collects information directly from you and from persons acting for an organizational Customer. NOVARC may also obtain information from:

- identity-verification, fraud-prevention, sanctions, PEP, adverse-media and blockchain-analytics providers;
- banks, payment processors, custodians, liquidity providers, virtual asset service providers and transaction counterparties;
- corporate registries, regulatory registers, courts, government databases and other public records;
- publicly available websites, professional networks and media sources where collection is appropriate and lawful;
- NOVARC affiliates, professional advisers, introducers and business partners where lawful and relevant to the relationship;
- another person involved in a transaction, including an originator, beneficiary or authorized representative.

Where information is collected from another source without your consent, NOVARC will do so only where permitted or required by applicable law.

7. Why We Collect, Use and Disclose Personal Information

NOVARC collects, uses and discloses Personal Information only for purposes that a reasonable person would consider appropriate in the circumstances. These purposes include:

- providing, administering, maintaining and improving the Platform and Services;
- processing applications, onboarding Customers, creating and managing approved profiles and authenticating users;
- preparing Quotes, confirming Orders, executing transactions, coordinating settlement and maintaining transaction records;
- verifying identity, authority, ownership, beneficial ownership, wallet control and bank account ownership;
- performing anti-money laundering and anti-terrorist financing controls, sanctions screening, fraud detection, wallet screening, travel rule compliance and ongoing transaction monitoring;
- assessing customer, transaction, geographic, product, operational, credit, financial crime and reputational risk;
- complying with legal, regulatory, record-keeping, reporting, tax, audit, court and law-enforcement requirements;
- preventing, detecting, investigating and responding to fraud, cyber incidents, misuse, disputes, chargebacks, unauthorized instructions and violations of NOVARC's terms or policies;
- communicating about onboarding, transactions, security, changes to Services, legal notices, support requests and complaints;
- conducting analytics, testing, quality assurance, business planning, service development and internal reporting;
- sending commercial communications with consent or as otherwise permitted by law;
- establishing, exercising or defending legal claims and carrying out a financing, reorganization, merger, acquisition or sale of business assets.

NOVARC will not use Personal Information for a new purpose that is materially different from the identified purposes unless NOVARC obtains any consent required by law or the use is otherwise permitted or required by law.

8. Consent and Other Lawful Authority

8.1 Meaningful consent

NOVARC obtains meaningful consent where required. Consent may be express, including through an acceptance box, signature, direct instruction or voluntary submission of information, or implied where the purpose is obvious to a reasonable person and the individual voluntarily provides the information for that purpose.

The form of consent will reflect the sensitivity of the information, the reasonable expectations of the individual and the significance of potential consequences. NOVARC may use a separate or more prominent notice when collecting Sensitive Information or using information for a purpose that may not be obvious.

8.2 Necessary and optional processing

NOVARC will not require consent to collection, use or disclosure beyond what is reasonably necessary to provide the requested Services, except where you choose an optional feature or communication. Some information is essential to identity verification, compliance, security, transaction execution and record keeping. NOVARC may be unable to provide or continue the Services if that information is not provided.

8.3 Withdrawal of consent

You may withdraw consent on reasonable notice, subject to legal or contractual restrictions. NOVARC will explain the likely consequences where appropriate. Withdrawal will not affect processing already lawfully completed and will not require NOVARC to delete information that must be retained or may continue to be used or disclosed without consent under applicable law.

8.4 Processing without consent

NOVARC may collect, use or disclose Personal Information without consent where permitted or required by law, including for investigations, fraud prevention, compliance with legal obligations, responding to lawful requests, debt collection, emergencies, business transactions, legal claims and other statutory exceptions.

9. AML/ATF, Sanctions and Regulatory Processing

NOVARC operates in a compliance-sensitive sector and may be required to collect, verify, retain, analyze and report Personal Information under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated regulations, sanctions laws, tax laws, court orders and other applicable requirements.

This processing may include identity and beneficial ownership verification, source-of-funds and source-of-wealth review, sanctions and PEP screening, adverse-media review, blockchain analytics, transaction monitoring, travel rule information exchange and regulatory reporting.

NOVARC may disclose information to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Bank of Canada where applicable, financial institutions, other financial intelligence units, regulators, sanctions authorities, law-enforcement agencies, courts and other competent bodies where required or permitted by law. NOVARC may be legally prohibited from telling you that a report, inquiry, investigation or disclosure has occurred.

10. Automated Tools, Screening and Risk Decisions

NOVARC and its Service Providers may use automated, rules-based or machine-assisted tools to support identity verification, document authentication, fraud detection, sanctions and PEP screening, adverse-media review, wallet risk analysis, transaction monitoring and security.

These tools may generate alerts, matches, risk indicators or scores. A match or score does not necessarily establish wrongdoing. Material onboarding, restriction or escalation decisions may be reviewed by authorized personnel where appropriate and reasonably practicable. NOVARC may request additional information or decline, delay, restrict or report activity where required by law or justified by compliance, security or risk considerations.

You may contact the Privacy Officer with questions about NOVARC's use of automated tools, subject to legal, security and confidentiality limitations.

11. Disclosure of Personal Information

NOVARC may disclose Personal Information only as reasonably necessary for the purposes described in this Policy and subject to appropriate safeguards. Recipients may include:

- identity-verification, document-authentication, sanctions, PEP, adverse-media, fraud and blockchain-analytics providers;
- banks, payment processors, card or payment networks, custodians, liquidity providers, virtual asset service providers, counterparties and settlement providers;
- cloud hosting, cybersecurity, communications, customer-support, analytics and technical service providers;
- NOVARC affiliates where necessary to provide Services, manage risk, support operations or comply with law, subject to appropriate arrangements;
- auditors, accountants, lawyers, insurers, consultants and other professional advisers;
- prospective or completed financing, restructuring, merger, acquisition or sale counterparties, subject to confidentiality and legal requirements;

- FINTRAC, the Bank of Canada where applicable, privacy commissioners, tax authorities, regulators, financial intelligence units, law enforcement, courts, sanctions authorities and other competent bodies where required or permitted by law;
- other parties with your consent, at your direction or where reasonably necessary to protect NOVARC, a Customer or another person from fraud, security threats or unlawful activity.

Service Providers are expected to process information only for authorized purposes and to use contractual, organizational and technical safeguards appropriate to the sensitivity of the information. NOVARC does not sell or rent Personal Information to third parties for their independent marketing purposes.

12. International and Cross-Border Processing

NOVARC and its Service Providers may process, access or store Personal Information outside British Columbia or Canada, including in jurisdictions where NOVARC affiliates, financial institutions, liquidity providers, identity-verification providers, cloud providers or other Service Providers operate.

Information processed in another jurisdiction may be subject to the laws of that jurisdiction and may be accessible to courts, regulators, law-enforcement or national-security authorities under those laws. The privacy protections and legal remedies available in another jurisdiction may differ from those in Canada.

NOVARC uses reasonable contractual, technical and organizational measures to protect information transferred across borders. You may contact the Privacy Officer for general information about relevant Service Provider locations and safeguards, subject to legal, contractual and security limitations.

13. Cookies and Similar Technologies

NOVARC may use cookies, local storage, pixels, software development kits and similar technologies for the following purposes:

- essential website operation, authentication, session management and transaction security;
- fraud prevention, traffic management and protection against abuse or cyber threats;
- remembering preferences and improving user experience;
- analytics, performance measurement, testing and service improvement;
- marketing or attribution where used and where consent is required.

You can control many cookies through your browser settings and, where available, the website consent tool. Blocking essential cookies may prevent parts of the Platform from functioning. Third-party tools may set their own cookies in accordance with their privacy notices.

NOVARC will obtain any consent required by applicable law before using non-essential technologies. More detailed information may be provided in a separate Cookie Notice or consent interface.

14. Retention and Disposal

NOVARC retains Personal Information only for as long as reasonably necessary for the purposes described in this Policy and to meet legal, regulatory, contractual, audit, dispute, limitation-period, security and business-continuity requirements.

Records subject to anti-money laundering, anti-terrorist financing or money services business requirements may be retained for at least five years, or longer where required by law, a regulator, a litigation hold, an investigation or another lawful requirement. Different periods apply depending on the record type, Customer status, transaction history and the reason for retention.

Where an application is not approved or a proposed transaction is not completed, NOVARC may retain relevant onboarding, screening and decision records for compliance, fraud prevention, audit, dispute and legal purposes.

When information is no longer required, NOVARC securely deletes, destroys or anonymizes it, subject to technical limitations, backup cycles and lawful retention obligations. Information recorded on a public blockchain generally cannot be deleted or altered by NOVARC.

15. Security Safeguards

NOVARC uses administrative, technical and physical safeguards that are reasonable and appropriate having regard to the sensitivity, volume, format, location and risk of the information. Measures may include:

- role-based access controls, confidentiality obligations, background screening where appropriate and staff training;
- encryption in transit and at rest where appropriate, secure configuration and key-management controls;

- multi-factor authentication, monitoring, logging, vulnerability management and security testing;
- vendor due diligence and contractual privacy and security requirements;
- incident response, business continuity, backup and secure-disposal processes;
- physical access controls for facilities, records and devices where applicable.

No method of electronic transmission or storage is completely secure. You are responsible for protecting your credentials, devices, email account, External Wallets and communication channels and for promptly reporting suspected compromise or unauthorized instructions.

16. Privacy and Security Incidents

NOVARC maintains procedures to identify, assess, contain, investigate and remediate suspected loss of, unauthorized access to, or unauthorized disclosure of Personal Information.

Where PIPEDA or another applicable law requires, NOVARC will notify the appropriate privacy commissioner and affected individuals of a breach of security safeguards that creates a real risk of significant harm. NOVARC will also notify other organizations or government institutions where legally required or where doing so may reduce the risk of harm. Required breach records will be maintained for the applicable retention period.

Even where notification is not legally mandatory, NOVARC may provide notice where it considers notification appropriate in the circumstances.

17. Your Privacy Rights

Subject to applicable law and permitted exceptions, you may:

- request access to Personal Information under NOVARC's control and information about how it has been used or disclosed;
- request correction of inaccurate or incomplete Personal Information;
- withdraw consent where processing is based on consent;
- ask questions or submit a complaint about NOVARC's privacy practices;
- unsubscribe from commercial electronic messages while continuing to receive necessary transactional, security, compliance and legal communications.

17.1 How to make a request

Send a written request to privacy@novarc.global. Please describe the request in sufficient detail and do not send passwords, private keys or complete payment credentials. NOVARC may require information to verify your identity and authority before responding.

17.2 Response and permitted limitations

NOVARC will respond within the period required by applicable law and may extend the response period where legally permitted. A reasonable fee may apply only where authorized by law and disclosed in advance.

Access may be restricted where disclosure would reveal another person's information, confidential commercial information, privileged material, security-sensitive information, information generated in a formal dispute-resolution process or information that NOVARC is prohibited by law from disclosing. Where permitted, NOVARC will explain the reason for a refusal or redaction and available complaint options.

17.3 Correction

Where NOVARC agrees that Personal Information is inaccurate or incomplete, it will correct the information as appropriate and may provide the corrected information to a party that received the inaccurate information where required by law. Where NOVARC does not make a requested correction, it may annotate the record with the unresolved request where appropriate.

18. Commercial Communications

NOVARC may send marketing or promotional communications only with consent or as otherwise permitted by applicable law. Messages will identify NOVARC and include an unsubscribe mechanism where required. Unsubscribe requests will be processed within the legally required period.

Unsubscribing from marketing does not prevent NOVARC from sending transaction confirmations, security alerts, compliance requests, legal notices or other communications necessary to provide or administer the Services.

19. Children and Minors

The Services are not directed to persons under the age of majority in their jurisdiction, and NOVARC does not knowingly provide Services to minors. If NOVARC learns that it collected Personal Information from an ineligible minor, it will take reasonable steps to delete the information unless retention is required or permitted by law.

20. Public Blockchains and Third-Party Services

20.1 Public blockchains

Public blockchains are generally transparent, distributed and immutable. Wallet addresses, transaction hashes, amounts, timestamps and related data may remain publicly available indefinitely and ordinarily cannot be deleted, corrected or altered by NOVARC. Information recorded on a blockchain may be linked to an identifiable individual through other information.

20.2 Third-party websites and services

The Platform may link to or integrate third-party websites, wallets, payment methods, market-data services or other services. Their privacy practices are governed by their own notices. NOVARC is not responsible for the privacy, security or content practices of an independent third party.

21. Changes to This Policy

NOVARC may update this Policy to reflect changes in law, Services, technology, risk or business practices. The current version will be posted on the Platform with its effective date. Where required, NOVARC will provide additional notice or obtain renewed consent for a material change.

Your continued use of the Platform after an updated Policy takes effect does not replace any consent that must be obtained separately under applicable law.

22. Contact and Complaints

Questions, access or correction requests, consent withdrawals and complaints should be directed to the Privacy Officer:

PRIVACY OFFICER	NOVARC Privacy Officer
PRIVACY EMAIL	privacy@novarc.global
LEGAL EMAIL	legal@novarc.global
REGISTERED OFFICE	C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada
WEBSITE	https://novarc.global/canada

NOVARC will investigate privacy complaints and communicate the outcome within a reasonable period. If you are not satisfied with NOVARC's response, you may contact the Office of the Information and Privacy Commissioner for British Columbia or the Office of the Privacy Commissioner of Canada, depending on which law applies to the matter.