Privacy Policy

Handling personal information in NOVARC services

EFFECTIVE DATE	15 October 2026
VERSION	2.0
LEGAL ENTITY	**NOVARC FINANCIAL LTD.**
INCORPORATION NO.	BC1579964
FINTRAC MSB	N300001947
REGISTERED OFFICE	C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada
WEBSITE	https://novarc.global/canada

I. Definitions

This Privacy Policy (the "Policy") explains the personal-information practices of NOVARC FINANCIAL LTD. ("NOVARC", "we", "our" or "us"), a company incorporated under the laws of British Columbia, Canada, under incorporation number BC1579964. Its registered office is C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada. We explain below how information is obtained, used, shared, retained and protected when an individual deals with NOVARC, requests a Service or accesses its website or related digital interfaces.

Personal Information means information relating to an identified or reasonably identifiable natural person, whether considered alone or together with other available records. **Customer** means an individual or organization using, applying for or interacting with NOVARC's Services; where an organization is involved, its directors, owners, representatives, employees and transaction counterparties may also be data subjects. **Services** means the digital asset, exchange, payment-related and ancillary activities made available by NOVARC from time to time.

Consent means a person's express or implied permission for an identified processing purpose, where applicable privacy law permits or requires that approach. **Service Provider** means an outside party supporting NOVARC's operations, for example a verification, banking, payment, hosting, security or analytics business. **Cookies** includes browser cookies, pixels, locally stored identifiers and functionally comparable technologies.

Non-Custodial Model refers to a transaction-oriented service in which NOVARC does not routinely keep an ongoing client deposit balance or custody wallet and does not manage a Customer's private keys as a continuing investment or deposit service. For an approved Order, operational settlement accounts or technical wallets may nevertheless be used temporarily if lawful and necessary. **OTC Transaction** is a negotiated transaction arranged directly with an eligible counterparty rather than necessarily executed through a public order book.

II. Privacy Laws and Lawful Handling

NOVARC seeks to handle Personal Information in accordance with the British Columbia Personal Information Protection Act ("BC PIPA") and, for commercial interprovincial or international processing and other activities within its scope, the federal Personal Information Protection and Electronic Documents Act ("PIPEDA"). Other jurisdiction-specific privacy obligations may apply to particular individuals or processing arrangements. This Policy is not intended to diminish a right granted by applicable legislation.

We ordinarily request meaningful consent for collection, use and disclosure of Personal Information unless an exception or another lawful authority allows or requires the relevant activity. Collection and processing must have legitimate, identified purposes that a reasonable person would consider suitable in the circumstances. We apply accountability, proportional collection, privacy-by-design measures and safeguards reflecting the sensitivity of the data.

III. Aim and Transparency of This Policy

The purpose of this Policy is to explain what types of Personal Information may be needed to provide the Services, from where that information comes, the reasons it is processed and the situations in which it can reach third parties or regulatory bodies. It also describes retention practices, security precautions and the methods available to individuals who want to ask a question, raise a concern or exercise access or correction rights.

Providing a general privacy notice does not remove the obligation to give more specific information or obtain separate consent when required for a particular new or sensitive processing activity. Transaction instructions, due-diligence questionnaires, website notices and a consent tool may therefore provide further details at the point of collection.

IV. Coverage of This Policy

The Policy covers information processed in connection with visits to our website, customer registration, business onboarding, identity and corporate verification, email or telephone correspondence, virtual currency and fiat exchange requests, OTC Quotes and Orders, settlement instructions, technical support, security reviews, AML/ATF monitoring and ordinary commercial dealings with NOVARC.

It covers both applicants and existing Customers and individuals acting for a corporate Customer, including beneficial owners, directors, authorized signatories, representatives, counterparties, originators and beneficiaries. It also applies to Personal Information that authorized Service Providers process on NOVARC's behalf. The location of a person or provider may affect which specific statutory duties apply.

Truly anonymized or irreversibly aggregated information that cannot reasonably identify a natural person is outside this definition of Personal Information. Certain professional contact details can be excluded from a particular statutory definition, but NOVARC may continue to handle them responsibly as a matter of operational practice.

V. Privacy Principles Followed by NOVARC

- **Accountability.** NOVARC accepts responsibility for information under its control and appoints a Privacy Officer to oversee compliance, staff procedures and inquiries.
- **Clarity of purpose.** Before or when information is collected, we identify material purposes and make additional disclosures where an unusual purpose is introduced.
- **Meaningful consent.** Where consent is necessary, we seek it in a form that reflects the sensitivity and reasonable expectations involved.
- **Proportionate collection.** We aim to request the information reasonably needed for an identified service, regulatory obligation or risk decision, rather than unrelated data.
- **Controlled use and retention.** Personal Information is not repurposed or retained indefinitely without an appropriate legal or business reason.
- **Accuracy.** Reasonable steps are taken to verify and update information where an inaccurate record could affect an important decision.
- **Protection.** Organizational, physical and technical safeguards are selected to reduce the foreseeable risk of unauthorized access, loss or misuse.
- **Openness.** Customers can obtain an explanation of our privacy practices and the route for reaching the Privacy Officer.
- **Individual access and correction.** Requests to see or amend information are addressed under the applicable statutory framework.
- **Review of concerns.** Privacy complaints are assessed and, where appropriate, acted upon through an internal review process.

VI. Types and Sources of Personal Information

The categories below reflect the kinds of information that may be processed, not a statement that every category is requested from every Customer. The information actually needed depends on the product, risk profile, jurisdiction, transaction structure and applicable legal obligations.

Identification and KYC Information

- Legal name, previous names or aliases, date of birth, citizenship, nationality, tax residence and residential address.

- Government identity documents, issuing country or authority, document details, validity dates and verification results.
- Photographs, selfie or liveness verification results and, if lawfully collected by an identity-checking provider, limited biometric-derived verification information.
- Occupation, role, employer or other background details needed to establish identity, capacity and eligibility.

Corporate, Contact and Authority Details

- Email address, telephone number, mailing details, preferred contact method and correspondence history.
- Legal or trading name, incorporation jurisdiction and number, directors, officers, authorized representatives and ownership or control records.
- Corporate charts, beneficial owner identification, resolutions, powers of attorney, regulatory registrations, operating descriptions and expected customer or transaction profile.

Payment, Financial and Transaction Records

- Payment and settlement instructions, eligible bank account identifiers, permitted payment-method details, proof of account ownership and transaction confirmations.
- Proposed and completed Quotes or Orders, asset amounts, fees, exchange rates, currencies, payment timestamps, associated counterparties and account or transaction references.
- Source-of-funds, source-of-wealth or anticipated-activity records when requested for financial-crime controls.

Virtual Currency and Blockchain Information

- Blockchain wallet addresses, network identifiers, transaction hashes, timestamps, blockchain movements and supported asset types.
- Evidence of wallet ownership or control where necessary, originator and beneficiary details, and screening or analytics results linked to a specific wallet or flow of virtual currency.

Technical, Security and Correspondence Information

- Internet Protocol addresses, device or browser details, login events, time-zone or approximate location indicators, diagnostic records and usage logs.
- Cookie identifiers, fraud-detection telemetry, service requests, customer service messages, complaints and optional communications preferences.

Compliance Information and External Sources

NOVARC may collect identity-checking and risk information from reliable verification companies, payment providers, banks, blockchain analytics businesses, regulators, corporate registries, lawful public records and transaction counterparties. Such information may include sanctions and politically exposed person matches, adverse media, suspected fraud indicators, regulatory status, beneficial ownership and enhanced due-diligence records. Information from an external source is requested or used only where there is an appropriate legal basis and it is relevant to an identified purpose.

VII. Purposes, Consent and Permitted Use

Operating the Services

NOVARC may use information to review applications, create and maintain an approved profile, authenticate users, prepare exchange Quotes, accept or decline Orders, process fiat or virtual currency exchanges, coordinate settlement, resolve failed transfers and communicate relevant transaction details. Processing may also support service maintenance, business administration, quality assurance and lawful product improvement.

KYC, AML/ATF and Compliance

Identity and beneficial ownership checks, sanctions screening, politically exposed person reviews, source-of-funds inquiries, wallet analytics, travel-rule information sharing, monitoring and regulatory record keeping may be required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA"), associated regulations and other applicable laws. NOVARC may make mandatory reports and respond to lawful requests from FINTRAC or another competent authority without obtaining a separate consent when legal rules permit or require the disclosure.

Fraud Prevention, Operational Risk and Security

We may analyze transactions, device behavior, identity information and payment patterns to identify suspected crime, unauthorized account activity, cyber incidents, chargeback abuse or misuse of the Platform. Such information can also help prevent harm, investigate a dispute, recover a legitimate debt or establish, exercise or defend legal rights where the relevant use is authorized by law.

Customer Relations and Improvements

We use contact details for onboarding messages, transaction updates, complaint management, important security notices and support. We may review aggregated usage patterns to improve performance, detect faults and develop new features. Optional commercial electronic messages are sent only with a lawful basis, including consent where required, and the ability to unsubscribe as prescribed by law.

How Consent Works

Where law calls for consent, it may be given through a signed instruction, a clearly worded online acceptance, a voluntary submission or another appropriately documented step. Implied consent is relied on only when legally available and reasonably understandable in context. We give particular consideration to the sensitivity of government IDs, financial records and verification information. Consent for optional marketing or non-essential tracking is treated separately when required.

You may withdraw consent on reasonable notice, subject to applicable legal or contractual restrictions. A withdrawal may prevent us from providing a requested Service, but it does not undo processing that was previously lawful or oblige us to erase records needed for compliance, investigations or another permissible purpose. We will explain significant practical consequences when appropriate.

VIII. When Personal Information Is Disclosed

Operational Providers and Counterparties

Information can be supplied on a limited, purpose-related basis to outsourced identity and document-verification firms, sanctions and blockchain-screening providers, banks, payment processors, custodians used for an individual settlement, liquidity providers, cloud hosts, cybersecurity services, technical vendors and approved transaction counterparties. NOVARC seeks arrangements requiring confidential handling, limited authorized use and appropriate security protections. NOVARC does not sell or rent Personal Information for an independent third party's marketing.

Authorities and Lawful Requests

We may provide records to FINTRAC, law-enforcement bodies, courts, tax agencies, sanctions officials, privacy commissioners, other financial regulators and competent government authorities where permitted or compelled by law. A statutory prohibition may prevent NOVARC from disclosing the existence or details of a report or investigation. The Bank of Canada may receive information if and to the extent NOVARC is subject to the RPAA and a legally relevant disclosure applies.

Affiliates, Professional Advisers and Business Transactions

Relevant information may be accessible to NOVARC affiliates, auditors, insurers, legal advisers, accountants and other professionals when reasonably necessary and lawful. In a merger, acquisition, financing or business transfer, limited due-diligence or transition disclosures may occur under confidentiality and other protections required by applicable privacy legislation. We may also share information on the instruction of the person concerned or with legally sufficient consent.

Transfers Across Borders

Some recipients may store, process or access Personal Information outside Canada or British Columbia. A foreign jurisdiction may apply different privacy rules and may allow its courts or public authorities to obtain access. NOVARC seeks proportionate contractual and technical safeguards; additional information on these arrangements may be requested from the Privacy Officer, subject to confidentiality and security considerations.

IX. Retention, Record Keeping and Disposal

We do not set a single retention period for every data category. Retention depends on the original purpose, the type of record, whether a Customer was onboarded, the timing of the last transaction, applicable statutory periods, record-keeping rules, potential disputes and legitimate security or audit needs.

Where AML/ATF legislation imposes prescribed record-keeping periods, relevant documents may need to be kept for five years or for another applicable period calculated from the statutory trigger. Longer preservation may be lawful or required during litigation, an audit, regulatory review or an investigation. Information from an unsuccessful onboarding or an incomplete transaction may also be retained when lawfully necessary for compliance or fraud prevention.

When the relevant lawful need ends, NOVARC takes appropriate steps to securely destroy, anonymize or otherwise dispose of records, taking account of backup schedules and technical constraints. Public blockchain entries, including addresses and transaction references, are generally not controlled by NOVARC and may remain visible or immutable after an account is closed.

X. Security and Incident Management

NOVARC seeks to use safeguards appropriate to the sensitivity and risks of the Personal Information concerned. These may include restricted system permissions, confidentiality duties, staff training, secure transmission, encryption where appropriate, multi-factor authentication, system monitoring, security testing, vendor assessments, incident-response procedures, backup controls and secure disposal practices.

Access is limited to personnel and authorized contractors whose duties justify it. NOVARC assesses suspected loss, inappropriate access or unauthorized disclosure and takes steps to contain, investigate and remediate incidents. Notices to individuals, the Office of the Privacy Commissioner of Canada, the British Columbia privacy commissioner or another authority will be made where legally required. Applicable breach-record obligations are respected.

No online service or data transfer is guaranteed to be invulnerable. Customers should protect their passwords, devices, email accounts, private keys and recovery credentials and report suspected compromise promptly. NOVARC will not ask you to disclose a wallet recovery seed phrase through an ordinary support request.

XI. Requests for Access and Correction

An individual may request access to Personal Information under NOVARC's control and, where legally available, details of its use or disclosure. Requests can be sent to privacy@novarc.global with enough information to locate the relevant records. To protect other individuals, we may ask for identification or proof that a representative is authorized before releasing data.

You may ask that incomplete or inaccurate information be corrected. Where a correction is justified, we will update the relevant records and notify recipients if legally required. If a dispute about accuracy cannot be resolved, the relevant record may be annotated where appropriate.

NOVARC will respond within applicable statutory time limits and may rely on lawful extensions, permitted fees or exceptions, including protection of another person's information, legal privilege, confidential commercial records, investigation confidentiality and information whose release is prohibited by law. If we lawfully refuse or limit access, we will explain the decision and available review route where allowed.

XII. Cookies, Tracking and Website Analytics

The website and digital interfaces may employ necessary cookies and similar tools for login, security, fraud detection, session continuity and basic operation. Other technologies may support preference settings, traffic statistics, diagnostics, usability improvements or attribution if used in the relevant product.

Technical information collected through these tools can include IP addresses, device and browser parameters, pages visited, identifiers, approximate location, events and access timestamps. External providers of hosting, security and analytics technology may operate their own tools under contractual restrictions and applicable law.

Most browsers allow you to refuse or remove many cookies. Where available, the NOVARC consent interface may permit additional choices. Non-essential cookies are subject to any legally required prior notice or consent. Blocking essential cookies may make certain Service functions unusable.

XIII. International Information Handling

NOVARC may rely on global cloud infrastructure, verification specialists, financial intermediaries and counterparties in jurisdictions outside Canada. This means information can be accessed, hosted or transferred to countries with privacy regimes and law-enforcement access rules different from those in British Columbia.

Where personal information is entrusted to overseas organizations, NOVARC takes steps appropriate to the circumstances, such as provider due diligence, confidentiality and processing clauses, restricted permissions and technological security measures. You may ask our Privacy Officer for general information about material international processing practices, subject to lawful limits on the disclosure of sensitive infrastructure or commercially protected information.

XIV. Privacy Officer, Requests and Complaints

NOVARC designates a Privacy Officer to coordinate its privacy-management practices, consider access and correction requests, respond to complaints and facilitate appropriate improvement of procedures. For questions about this Policy or how your information is used, please write to privacy@novarc.global. General legal correspondence may be sent to legal@novarc.global.

Please describe your concern and the records involved without emailing passwords, wallet seed phrases or complete payment credentials. We aim to investigate and answer privacy complaints within a reasonable period and in all cases within any binding statutory deadline.

If a matter cannot be resolved internally, you may be entitled to bring a complaint to the Office of the Information and Privacy Commissioner for British Columbia or the Office of the Privacy Commissioner of Canada, depending on the applicable legislation. Nothing in this Policy restricts statutory access, correction, complaint or other non-waivable privacy rights.

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

XV. Amendments and Effective Date

NOVARC may change this Policy when its Services, data handling, technology, legal obligations or risk procedures evolve. The current version will state an effective date and be made available on the website. Where a change requires additional notice or a new consent, NOVARC will follow the relevant legal requirement rather than relying solely on continued use of the Platform.

This Policy takes effect on 15 October 2026. Older versions may remain relevant to processing that occurred before a revised version became effective, and a subsequent update will not retrospectively remove any mandatory rights.