Privacy Policy

How NOVARC USA collects, uses, discloses and protects personal information

EFFECTIVE DATE	16 July 2026
VERSION	1.0
COMPANY	**NOVARC FINANCIAL LTD. - Montana, United States**
MONTANA CERTIFIED FILE NO.	**D1644130-17257259**
BUSINESS ADDRESS	1001 S. Main St. #7006, Kalispell, Montana 59901, United States
FINCEN MSB REGISTRATION	**No. 31000332452909 - money transmitter**
WEBSITE	https://novarc.global/usa

Privacy questions and requests: privacy@novarc.global

1. Who We Are

NOVARC FINANCIAL LTD. is a Montana domestic profit corporation formed under the laws of the State of Montana. The Montana Secretary of State certification became effective on May 28, 2026, under Certified File Number D1644130-17257259. Its business address is 1001 S. Main St. #7006, Kalispell, Montana 59901, United States. In this Policy, "NOVARC", "we", "us" and "our" refer only to this Montana corporation.

NOVARC is registered with the Financial Crimes Enforcement Network of the U.S. Department of the Treasury ("FinCEN") as a money services business ("MSB") under registration number 31000332452909. The registration identifies money transmission as the MSB activity and Montana as the state of MSB activity. FinCEN registration is not a banking charter, state money transmitter license, government approval, recommendation, endorsement or guarantee.

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

2. Scope and Applicable Privacy Framework

This Policy applies to Personal Data collected, used, disclosed or otherwise processed through the NOVARC USA 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 visit, apply for or 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.

Depending on the individual, information and activity, NOVARC may be subject to the Gramm-Leach-Bliley Act ("GLBA") and the FTC Privacy Rule, the FTC Safeguards Rule, the Federal Trade Commission Act, the Bank Secrecy Act ("BSA"), the USA PATRIOT Act, FinCEN regulations, sanctions administered by the Office of Foreign Assets Control ("OFAC"), the Montana Consumer Data Privacy Act ("MCDPA"), state data-breach notification laws and other federal or state requirements.

Some laws apply only when statutory thresholds, residency, customer type or product conditions are met. Certain information processed in accordance with GLBA, BSA, anti-money laundering, fraud prevention, legal claims or other regulated activities may be exempt from some state privacy rights. Where another jurisdiction applies, NOVARC may provide a supplemental notice or apply additional rights and safeguards.

This Policy does not apply to anonymized or aggregated information that cannot reasonably be linked to an identifiable individual, or to information excluded from the definition of Personal Data under applicable law.

3. Key Definitions

Personal Data: information that is linked or reasonably linkable to an identified or identifiable individual. The term includes nonpublic personal information where GLBA applies and excludes de-identified or publicly available information to the extent provided by law.

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 Data: data that is treated as sensitive under applicable law, which may include government identification, authentication credentials, financial account information, precise geolocation, biometric identifiers, citizenship or immigration status, and information revealing protected characteristics.

Service Provider: a third party that processes data or supports NOVARC operations, including identity-verification, banking, payment, liquidity, custody, blockchain analytics, fraud prevention, cloud, security, communications and professional service providers.

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

Sale: the exchange of Personal Data for monetary or other valuable consideration where the term is defined by applicable state law, excluding statutory exceptions such as disclosures to processors, at the consumer's direction, or in a corporate transaction.

4. Privacy at a Glance and Notice at Collection

What we collect	Identity, corporate ownership, contact, financial, transaction, wallet, blockchain, compliance, communications, device and security information.
Why we use it	To onboard and verify Customers, provide and secure the Services, execute and settle transactions, comply with BSA/AML and sanctions obligations, prevent fraud and manage risk.
Who receives it	Service Providers, financial institutions, transaction counterparties, NOVARC affiliates, professional advisers and government authorities where necessary or lawful.
Sale and targeted advertising	NOVARC does not sell Personal Data or process it for targeted advertising as those terms are defined by applicable state privacy law. If this practice changes, NOVARC will update this Policy and provide any required opt-out.
Retention	Information is kept only for legitimate business and legal purposes. BSA, FinCEN and related records may be retained for at least five years or longer where required.
Your rights	Depending on applicable law, you may request access, correction, deletion or a portable copy, withdraw consent, appeal a decision and opt out of certain processing.

No private keys

NOVARC will not ask you to disclose a private key, wallet seed phrase or complete password. Do not send those credentials by email, chat, form or telephone.

5. Personal Data We Collect

The categories collected depend on the Services requested, Customer type, transaction, applicable law, NOVARC 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, tax residence and occupation;
- government-issued identification, document numbers, issuing authority, expiration date and verification results;
- photographs, selfies, liveness checks, facial comparison results and biometric identifiers where used by an identity-verification provider and permitted by law;
- Social Security number, taxpayer identification number or similar identifier where required for verification, tax, reporting or compliance purposes.

5.2 Business, authority and beneficial ownership information

- legal and trading names, jurisdiction, formation or registration number and registered, principal or business address;
- directors, officers, authorized representatives, shareholders, partners, trustees and ultimate beneficial owners;
- ownership and control charts, corporate records, licenses, regulatory status and nature of business;
- authority documents, expected activity, counterparties, geographic exposure and source of funds or source of wealth.

5.3 Financial, transaction and blockchain information

- bank account, routing, payment and beneficiary information, payment status and transaction history;
- Quotes, Orders, amounts, currencies, fees, timestamps, settlement instructions and transaction confirmations;
- wallet addresses, transaction hashes, network information, blockchain activity and proof of wallet ownership or control;
- blockchain analytics, wallet risk indicators and exposure to sanctioned, stolen, illicit or high-risk services;

- chargeback, reversal, dispute, refund, recovery and error-resolution information.

5.4 Contact, communications and support information

- email address, telephone number, mailing or business address and communication preferences;
- messages, inquiries, complaints, support interactions, call notes and transaction instructions;
- information provided through forms, meetings, onboarding questionnaires or due-diligence requests.

5.5 Technical, device and usage information

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

5.6 Sensitive Data and biometric information

Sensitive Data is collected only where reasonably necessary for verification, security, compliance, transaction execution or another disclosed purpose. Where a law requires consent before processing Sensitive Data or biometric identifiers, NOVARC or the relevant Service Provider will obtain the required consent or use another lawful exception. Biometric and liveness information is not used for advertising and is retained only for the period permitted by law and operational requirements.

6. Sources of Personal Data

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

- identity-verification, document-authentication, fraud prevention, sanctions, PEP, adverse-media and blockchain analytics providers;
- banks, payment processors, liquidity providers, custodians, virtual asset service providers and other transaction counterparties;
- corporate registries, regulatory registers, courts, government databases, sanctions lists and public records;
- publicly available websites, professional networks and media sources where lawful and relevant;
- NOVARC affiliates, professional advisers and business partners where lawful and relevant to the relationship;
- devices, browsers, cookies and security systems when you use the Platform.

Where information is obtained from another source, NOVARC may combine it with information received directly from you for verification, security, compliance, transaction and risk-management purposes.

7. Why We Collect, Use and Disclose Personal Data

NOVARC processes Personal Data for legitimate and disclosed business purposes, including:

- providing, administering, maintaining and improving the Platform and Services;
- processing applications, onboarding Customers, 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 BSA/AML, sanctions, fraud, wallet and transaction screening, travel rule compliance and ongoing monitoring;
- assessing customer, transaction, geographic, product, operational, credit, financial crime and reputational risk;
- complying with legal, regulatory, recordkeeping, reporting, tax, audit, subpoena, court and law-enforcement requirements;
- preventing, detecting, investigating and responding to fraud, cyber incidents, misuse, disputes, chargebacks and unauthorized instructions;
- 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 financing, reorganization, merger, acquisition or sale transactions.

NOVARC will not process Personal Data for a materially different and incompatible purpose unless the individual receives appropriate notice and NOVARC obtains any consent required by law or the processing is otherwise permitted by law.

8. Consent, Instructions and Other Lawful Processing

8.1 Consent and customer instructions

NOVARC obtains consent where applicable law requires it, including for certain Sensitive Data, biometric processing, optional communications or non-essential cookies. Consent may be provided through an acceptance box, signature, direct instruction, voluntary submission of information or another legally valid action.

8.2 Processing necessary for Services and compliance

Much of NOVARC's processing is necessary to verify identity and authority, prevent fraud, execute transactions, comply with BSA/AML and sanctions obligations, maintain required records and protect the Platform. NOVARC may be unable to onboard a Customer, execute an Order or continue a relationship if required information is not provided.

8.3 Withdrawal and revocation

Where processing is based on consent, you may withdraw or revoke consent through the method described at collection or by contacting the Privacy Officer. Revocation will be processed within the period required by applicable law. It does not affect processing already lawfully completed and does not require deletion of information that NOVARC must retain or may continue to process under law.

8.4 Legal exceptions

NOVARC may process or disclose Personal Data without consent where permitted or required by law, including for fraud prevention, investigations, compliance, legal process, sanctions, debt or loss recovery, emergencies, corporate transactions, security, legal claims and other statutory exceptions.

9. BSA/AML, OFAC and Regulatory Processing

As a registered MSB, NOVARC must maintain a risk-based anti-money laundering program and may be required to collect, verify, retain, analyze and report Personal Data under the BSA, FinCEN regulations, the USA PATRIOT Act, OFAC sanctions requirements and applicable state law.

This processing may include customer identification, beneficial ownership verification, source-of-funds and source-of-wealth review, sanctions and politically exposed person screening, adverse-media review, blockchain analytics, transaction monitoring, funds transfer recordkeeping, travel rule information exchange and regulatory reporting.

NOVARC may disclose information to FinCEN, OFAC, the Internal Revenue Service, the U.S. Department of Justice, federal or state regulators, financial institutions, law-enforcement agencies, courts and other competent authorities where required or permitted by law. NOVARC may be legally prohibited from telling you that a Suspicious Activity 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, potential 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 practical. NOVARC may request additional information or decline, delay, restrict or report activity where required by law or justified by compliance, security or risk considerations.

NOVARC does not currently use Personal Data for profiling in furtherance of automated decisions that produce legal or similarly significant effects as that term is defined by applicable state privacy law, except where necessary for fraud, security or compliance and permitted by law. If this changes, NOVARC will provide any required notice and opt-out.

11. Disclosure of Personal Data

NOVARC may disclose Personal Data 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, 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;
- FinCEN, OFAC, tax authorities, regulators, financial intelligence units, law enforcement, courts, attorneys general 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.

NOVARC does not sell or rent Personal Data to third parties for their independent marketing purposes. 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.

12. U.S. Financial Privacy Notice

This Section applies to the extent NOVARC provides a financial product or service to an individual primarily for personal, family or household purposes and the GLBA and FTC Privacy Rule apply. Business and institutional relationships may fall outside the GLBA consumer notice requirements, although NOVARC continues to protect the information under this Policy and applicable law.

NOVARC collects nonpublic personal information from applications, identity and corporate verification materials, transaction instructions, bank and wallet information, communications, Service Providers, financial institutions and public records. NOVARC may disclose this information for everyday business purposes permitted by law, including processing transactions, maintaining records, preventing fraud, complying with legal requirements and responding to regulators or law enforcement.

Process transactions, maintain records, prevent fraud and respond to legal process	NOVARC may share as permitted or required by law. A federal opt-out generally does not apply to these disclosures.
Marketing by NOVARC	NOVARC does not use nonpublic personal information for unrelated marketing without consent or another lawful basis.
Joint marketing with other financial companies	NOVARC does not currently share nonpublic personal information for joint marketing.
Affiliates' everyday business purposes	NOVARC does not currently share nonpublic personal information with affiliates for creditworthiness or unrelated everyday business purposes.
Nonaffiliates marketing to you	NOVARC does not share nonpublic personal information with nonaffiliates so they can independently market to you.
Former customers	NOVARC applies the same disclosure and safeguarding principles to former customers, subject to legal retention and reporting duties.

If NOVARC changes a practice in a manner that creates a federal right to limit sharing, NOVARC will provide a revised notice and a reasonable opt-out method before the new disclosure occurs, as required by law. NOVARC may provide a separate GLBA model privacy notice where operationally or legally appropriate; that notice supplements this Policy.

13. Cookies and Similar Technologies

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

- 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 or an opt-out is required.

You can control many cookies through 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 consent or recognize opt-out preference signals, including a legally recognized universal opt-out mechanism, where applicable law requires it. Because NOVARC does not currently sell Personal Data or use it for targeted advertising, such a signal should not materially change NOVARC's current processing, but NOVARC will honor it where legally required.

14. State Privacy Rights

Depending on your state of residence, the applicable law, statutory thresholds and available exemptions, you may have the right to:

- confirm whether NOVARC processes your Personal Data and access that data;
- correct inaccurate Personal Data;
- delete Personal Data, subject to legal and operational exceptions;
- obtain a copy of Personal Data you provided in a portable and readily usable format;
- opt out of the sale of Personal Data, targeted advertising or qualifying profiling;
- withdraw consent to the processing of Sensitive Data where consent is required;
- appeal NOVARC's refusal to act on a request;
- exercise rights without unlawful discrimination or retaliation.

14.1 Montana residents

Where the MCDPA applies, NOVARC will respond to an authenticated request without undue delay and generally within 45 days. NOVARC may extend the response period by up to 45 additional days where reasonably necessary and will explain the extension. If NOVARC declines a request, it will provide an explanation and instructions for appeal. NOVARC will generally decide an appeal within 60 days and, where required, provide a method to contact the Montana Attorney General.

14.2 Authorized agents and verification

You may use an authorized agent to exercise an opt-out right where applicable law permits. NOVARC may request proof of the agent's authority and may independently verify your identity. NOVARC will not disclose highly sensitive credentials, full identification numbers, financial account numbers, passwords or biometric data in response to an access request; instead, NOVARC may describe the categories collected with sufficient specificity.

14.3 Exceptions and limitations

Rights may be limited where information is governed by GLBA, BSA, FinCEN recordkeeping, sanctions, fraud prevention, legal process, litigation hold, security, trade-secret, confidential commercial, privileged or other statutory exceptions. A deletion request does not require NOVARC to delete blockchain records or data that must be retained by law.

15. How to Exercise Privacy Rights

Submit a request to privacy@novarc.global and describe the requested action and the state in which you reside. Do not send passwords, private keys, seed phrases or complete payment credentials. NOVARC may request information reasonably necessary to verify your identity, residency, authority and the scope of the request.

NOVARC will provide a response free of charge where required by law. If requests are manifestly unfounded, excessive, repetitive, fraudulent or technically infeasible, NOVARC may charge a reasonable fee or decline to act to the extent permitted by law. NOVARC will explain the reason and any appeal process.

To appeal a request decision, reply to the decision email with the word "APPEAL" in the subject line and explain why you believe the decision should be reconsidered.

16. Retention and Disposal

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

BSA, FinCEN, funds transfer, customer identification, transaction, registration and Suspicious Activity Report records may be retained for at least five years, and longer where required by law, a regulator, litigation hold, investigation, subpoena or other lawful requirement. Retention periods vary by record type, Customer status, transaction history and purpose.

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 de-identifies it, subject to backup cycles, technical limitations and lawful retention duties. Information recorded on a public blockchain generally cannot be deleted or altered by NOVARC.

17. 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. To the extent the FTC Safeguards Rule applies, NOVARC maintains a written information security program designed to protect customer information.

- designation of responsible personnel and risk-based security governance;
- role-based access controls, confidentiality obligations 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.

18. Privacy and Security Incidents

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

Where applicable law requires, NOVARC will notify affected individuals, the Montana Attorney General or another state authority, the Federal Trade Commission, FinCEN, law enforcement, Service Providers or other competent bodies. Notification content and timing depend on the nature of the information, the number and residence of affected individuals, whether the information was encrypted and the requirements of the applicable law.

Even where notification is not legally mandatory, NOVARC may provide notice where it considers notification appropriate to reduce the risk of harm.

19. Children and Minors

The Services are not directed to children or minors and are available only to persons who have reached the age of majority and are otherwise eligible under the Terms of Service. NOVARC does not knowingly provide money transmission or digital asset transaction Services to minors.

If NOVARC learns that it collected Personal Data from an ineligible minor, it will take reasonable steps to restrict and delete the information unless retention is required by law. NOVARC does not sell a minor's Personal Data, use it for targeted advertising or use profiling to make legally or similarly significant decisions. Where law requires parental or minor consent for a specific online processing activity, NOVARC will obtain the required consent or not conduct the activity.

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. Public blockchain data 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. International and Cross-Border Processing

NOVARC and its Service Providers may process, access or store Personal Data in the United States and other countries where NOVARC affiliates, banks, liquidity providers, identity-verification providers, cloud providers or other Service Providers operate.

Information processed in another country may be subject to local law and may be accessible to courts, regulators, law enforcement or national-security authorities. NOVARC uses reasonable contractual, technical and organizational measures to protect information transferred across borders. Individuals outside the United States may receive a supplemental notice where local law requires it.

22. 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.

23. 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 and last-updated date. Where required, NOVARC will provide additional notice or obtain consent before a material change applies to previously collected Personal Data.

A material change will apply prospectively unless applicable law permits otherwise. Continued use of the Platform does not replace any consent or opt-out opportunity that must be provided separately under law.

24. Contact, Requests and Complaints

Questions, privacy-rights requests, consent withdrawals, security concerns and complaints should be directed to the Privacy Officer:

PRIVACY OFFICER	NOVARC Privacy Officer
PRIVACY EMAIL	privacy@novarc.global
LEGAL EMAIL	legal@novarc.global
BUSINESS ADDRESS	1001 S. Main St. #7006, Kalispell, Montana 59901, United States
WEBSITE	https://novarc.global/usa
FINCEN MSB NO.	31000332452909

NOVARC will investigate privacy complaints and communicate the outcome within a reasonable period. If a state privacy-law appeal is denied, NOVARC will provide any regulator or attorney-general complaint information required by applicable law. Nothing in this Policy restricts your right to contact a competent government authority.