



PRIVACY POLICY

Last Updated: October 30, 2026

1. Introduction

1.1 This Privacy Policy ("**Policy**") describes how Nota Inc. ("**Nota**", "**we**", "**us**", or "**our**") collects, uses, discloses, and safeguards personal data when individuals interact with our website <https://notainc.co/> ("**Website**"), client portals, onboarding platforms, communication channels, or any of our Services (as defined in the Platform Terms and Conditions).

1.2 Nota Inc. is a corporation incorporated under the laws of Canada, corporation number 1000640793, with its registered office at 1110 Finch Avenue West, Suite 220, North York, Ontario, M3J 2T2, Canada. Nota is a registered Money Services Business (MSB) with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), registration number M23079093.

1.3 This Policy is designed to comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy legislation. Where the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the UK General Data Protection Regulation ("**UK GDPR**"), the Swiss Federal Act on Data Protection ("**FADP**") or other privacy legislation applies to Nota's processing of personal data, Nota processes such data in accordance with that legislation.

1.4 This Policy applies to Clients (both legal entities and individuals), their authorized representatives, directors, beneficial owners, beneficiaries, business partners, and Website visitors worldwide.

1.5 This Policy should be read together with the Platform Terms and Conditions, which govern the Services, and the Website Terms of Use, which govern the use of the Website. By accessing the Website or using any of our Services, you acknowledge that you have read and understood this Policy.

2. Data Controller

2.1 Nota is the data controller for personal data collected or processed in connection with its Services, including personal data relating to third parties provided by Clients (such as transaction beneficiaries). Nota independently determines the purposes and means of processing such data for compliance, fraud prevention, and regulatory reporting purposes. In limited circumstances where Nota processes personal data solely on a Client's documented instructions and for no independent purpose, Nota may act as a data processor under a written Data Processing Agreement.

2.2 Where the Client provides Nota with personal data relating to third parties (such as beneficiaries, directors, or beneficial owners), the Client acts as an independent data controller in respect of such data and is responsible for ensuring that it has obtained all necessary consents and provided all required notices to such individuals.

2.3 Nota's Data Protection Contact is the Director of Nota Inc. Inquiries regarding this Policy or the exercise of data subject rights may be directed to support@notainc.co.

3. Definitions

3.1 "**Personal Data**" means any information relating to an identified or identifiable natural person.

3.2 "**Processing**" means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

3.3 “**Data Subject**” refers to an individual whose personal data is processed.

3.4 “**Controller**” and “**Processor**” have the meanings ascribed to them under the GDPR, UK GDPR, and PIPEDA, as applicable.

3.5 Capitalized terms not defined in this Policy have the meanings given to them in the Platform Terms and Conditions.

4. Data We Collect

4.1 We may collect and process the following categories of personal data:

- (a) Identification data: name, date of birth, place of birth, nationality, gender, identification document details (passport, national ID, driver’s licence), photographs, signatures, and video recordings collected during identity verification;
- (b) Contact information: email address, telephone number, residential or business address, and messenger identifiers;
- (c) Financial and transactional information: bank account details, payment instrument details, transaction history, invoices, and payment records;
- (d) KYC/AML compliance data: source of funds and source of wealth documentation, occupation, corporate structure, beneficial ownership information, sanctions and PEP screening results, and risk assessment outcomes;
- (e) Corporate data (for legal entity Clients): corporate registration documents, articles of incorporation, shareholder registers, and information relating to directors, officers, trustees, and beneficial owners;
- (f) Technical and usage data: IP address, device identifiers, browser type and version, operating system, access times, pages visited, referral URLs, and interaction data;
- (g) Communication records: emails, chat messages, recorded calls (where permitted by law), and correspondence through any communication channel used in the course of the business relationship; and
- (h) Other data: any additional information provided by the Client or collected in the course of providing the Services, including information required for regulatory compliance.

4.2 Where Nota provides Services to individual Clients, the following additional categories of personal data may be collected:

- (a) selfie images or biometric verification data for identity confirmation;
- (b) device geolocation data (where enabled by the individual and required for fraud prevention);
- (c) employment and income information; and
- (d) additional documentation as required for compliance purposes.

4.3 This list is non-exhaustive. Nota may collect additional categories of personal data as required to provide its Services or comply with applicable law.

4.4 Biometric data. Where identity verification is carried out in respect of an individual Client, or of a director, beneficial owner, authorized representative or other individual connected with a Client, Nota or its identity verification providers may process facial images, video recordings and biometric data derived from them, and Nota may receive such data or the results of its verification from those providers. Biometric data is processed only with the explicit consent of the individual concerned, solely for the purposes of verifying identity, preventing fraud and complying with applicable law, and is retained only for as long as necessary for those purposes and as required by applicable law.

5. Sources of Data

5.1 We obtain personal data:

- (a) directly from you during onboarding, account registration, and use of the Services, and when you book a call through the Website;
- (b) from corporate Clients providing data relating to their representatives, directors, and beneficial owners;
- (c) from public registers, corporate registries, sanctions lists, and government databases;
- (d) from third-party service providers performing identity verification, AML/CTF checks, or fraud prevention services;
- (e) automatically through your use of the Website and Services (technical and usage data); and
- (f) from regulatory and law enforcement authorities, where applicable.

6. Purposes and Legal Basis for Processing

6.1 We process personal data for the following purposes:

Purpose	Legal Basis (PIPEDA)	Legal Basis (GDPR/UK GDPR)
Onboarding, identity verification, and KYC/CDD	Consent; legal requirement	Legal obligation; performance of contract; explicit consent (biometric data)
Providing and executing the Services, including transaction processing	Consent; necessity for services	Performance of contract
AML/CTF compliance, sanctions screening, PEP checks, and regulatory reporting	Legal requirement	Legal obligation
Fraud prevention and detection	Reasonable purpose	Legitimate interests; legal obligation
Ongoing monitoring of Client relationships and enhanced due diligence	Legal requirement; reasonable purpose	Legal obligation; legitimate interests
Communication with Clients (operational)	Necessity for services	Performance of contract; legitimate interests
Arranging calls and responding to enquiries from prospective clients	Consent	Steps taken at your request prior to entering into a contract; legitimate interests
Improving the Website, Services, and user experience	Reasonable purpose	Legitimate interests
Website analytics and measuring the effectiveness of our advertising, through cookies	Consent	Consent
Responding to data subject requests and complaints	Legal requirement	Legal obligation
Pursuing or defending legal claims	Reasonable purpose	Legitimate interests
Complying with court orders, subpoenas, and law enforcement requests	Legal requirement	Legal obligation

6.2 Where processing is based on consent, you may withdraw your consent at any time by contacting us at support@notainc.co. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal. Withdrawal of consent may result in the suspension or termination of Services where the processing is necessary for service delivery or compliance.

6.3 Where processing is based on legitimate interests, we have conducted a balancing assessment to ensure that our interests do not override your fundamental rights and freedoms.

7. Data Sharing and Disclosure

7.1 We share personal data only as necessary for the purposes described in this Policy and in accordance with applicable law. Recipients of personal data may include:

- (a) Banking and payment partners: financial institutions, correspondent banks, and payment service providers involved in the execution of transactions;
- (b) Compliance and fraud prevention providers: entities providing identity verification, AML/CTF screening, sanctions monitoring, blockchain analytics, and transaction monitoring services;
- (c) Regulatory and government authorities: FINTRAC, the Bank of Canada, law enforcement agencies, tax authorities, and other competent authorities as required by law;
- (d) Professional advisors: lawyers, auditors, accountants, and consultants engaged by Nota;
- (e) Technology and infrastructure providers: hosting providers, cloud services, IT support, and software vendors involved in the operation of Nota's systems, scheduling tools used to book calls through the Website, and analytics and advertising providers in respect of information collected through cookies where you have consented to their use;
- (f) Nota's affiliates, subsidiaries, and parent entities; and
- (g) Other third parties: where disclosure is required by law, court order, or regulatory directive, or where necessary for the performance of Nota's obligations.

7.2 All recipients are bound by contractual confidentiality and data protection obligations. We do not sell personal data to third parties.

8. International Data Transfers

8.1 Nota operates internationally. Personal data may be transferred to, stored in, and processed in countries other than your country of residence, including countries that may not provide an equivalent level of data protection.

8.2 Where personal data is transferred outside of Canada, the EEA, the UK, or Switzerland, such transfers are safeguarded by appropriate mechanisms, including:

- (a) Standard Contractual Clauses (SCCs) approved by the European Commission;
- (b) the UK International Data Transfer Agreement (IDTA) or UK Addendum to the EU SCCs;
- (c) contractual arrangements that provide substantially similar protections as required under PIPEDA; or
- (d) other lawful transfer mechanisms recognized under applicable data protection legislation.

9. Data Retention

9.1 We retain personal data for as long as necessary to fulfill the purposes for which it was collected, to comply with applicable legal and regulatory obligations, and to protect Nota's legitimate interests.

9.2 Records related to AML/CTF compliance are retained for a minimum of five (5) years from the date of the Transaction or the end of the business relationship, whichever is later, in accordance with the PCMLTFA and FINTRAC requirements.

9.3 Where a longer retention period is required by applicable law, regulation, or court order, personal data will be retained for the duration of such obligation.

9.4 Personal data that is no longer required will be securely deleted or anonymized in accordance with Nota's data retention schedule.

10. Security Measures

10.1 Nota applies technical and organizational measures to protect personal data against unauthorized access, loss, alteration, or disclosure.

10.2 No method of transmission over the Internet or electronic storage is completely secure. Nota cannot guarantee the absolute security of personal data.

11. Automated Processing

11.1 Nota uses automated systems for sanctions screening, PEP checks, transaction monitoring, and fraud detection. Such processing may result in the flagging, delay, or rejection of transactions or the suspension of access to Services.

11.2 Automated processing for AML/CTF compliance purposes is carried out pursuant to Nota's legal obligations under the PCMLTFA and applicable regulations.

11.3 Where automated processing produces legal or similarly significant effects on you, you have the right to request human review of the decision by contacting support@notainc.co.

12. Rights of Data Subjects

12.1 Depending on your jurisdiction and applicable law, you may have the following rights in relation to your personal data:

- (a) Access: the right to obtain confirmation of whether we process your personal data and to receive a copy of such data;
- (b) Rectification: the right to request correction of inaccurate or incomplete personal data;
- (c) Erasure: the right to request deletion of your personal data, subject to applicable legal retention obligations;
- (d) Restriction: the right to request that we restrict the processing of your personal data in certain circumstances;
- (e) Portability: the right to receive your personal data in a structured, commonly used, machine-readable format and to request its transfer to another controller;
- (f) Objection: the right to object to processing based on legitimate interests or for direct marketing purposes;
- (g) Withdrawal of consent: the right to withdraw consent at any time where processing is based on consent; and
- (h) Automated decision-making: the right to contest decisions made solely by automated means that produce legal or similarly significant effects.

12.2 To exercise any of these rights, please contact us at support@notainc.co. We will respond to requests within the timeframes prescribed by applicable law.

12.3 Nota may request verification of your identity before processing a data subject request. Certain rights may be limited where Nota has an overriding legal obligation to retain or continue processing personal data.

13. Cookies and Tracking Technologies

13.1 Our Website uses cookies and similar tracking technologies. Details regarding the types of cookies used, their purposes, and how to manage your cookie preferences are set out in our Cookie Policy, available at <https://notainc.co/en/cookie-policy>.

14. Children's Data

14.1 Nota's Services are not directed at individuals under the age of 18. We do not knowingly collect personal data from persons under 18 years of age. If we become aware that we have collected personal data from a person under 18 without appropriate authorization, we will take steps to delete such data.

15. Accountability and Governance

15.1 Nota maintains internal data protection governance practices, including data protection impact assessments (DPIAs) where required and records of processing activities.

15.2 Nota's Data Protection Contact oversees compliance with this Policy and applicable data protection legislation.

16. Complaints and Supervisory Authorities

16.1 If you believe that your data protection rights have been violated, you may:

- (a) contact Nota at support@notainc.co;
- (b) for Canadian residents: file a complaint with the Office of the Privacy Commissioner of Canada (<https://www.priv.gc.ca>);
- (c) for EEA residents: file a complaint with your local data protection supervisory authority;
- (d) for UK residents: file a complaint with the Information Commissioner's Office (<https://ico.org.uk>); and
- (e) for Swiss residents: file a complaint with the Federal Data Protection and Information Commissioner (<https://www.edoeb.admin.ch>).

17. Updates to This Policy

17.1 We may update this Policy from time to time. Updates will be posted on the Website with the revised "Last Updated" date indicated above.

17.2 Nota will provide reasonable advance notice of material changes to this Policy, where practicable. Continued use of the Services after such changes constitutes acceptance of the updated Policy.

18. Contact Information

Nota Inc.

1110 Finch Avenue West, Suite 220

North York, Ontario, M3J 2T2, Canada

Corporation number: 1000640793

MSB Registration (FINTRAC): M23079093

Email: support@notainc.co

Website: <https://notainc.co/>