NotaryPro Technologies Inc. – Privacy Policy

Last Updated: January 2026

1. Introduction

NotaryPro Technologies Inc. ("**NotaryPro**", **"we"**, **"us"** or **"our"**) recognizes the importance of privacy and is committed to protecting the personal information of our users. This **Privacy Policy** explains how we collect, use, disclose and safeguard your personal information when you use our websites (including **www.notarypro.ca**, **www.notarypro.com** and any associated subdomains), mobile applications and related services (collectively, the **"Platform"**). It supplements the **General Terms of Service**, the various **Service Supplements** referenced therein (e.g., the **Online Commissioning Supplement**, **AI Document Supplement** and **Business Services Supplement**), the Data Processing Supplement and the Security Statement, as well as the Affiliate & Reseller Agreement and, for biometric identifiers and biometric information **("Biometric Data"),** our Biometric Data Policy and Arbitration Agreement (collectively, the "Terms"). This Policy forms part of your agreement with us. By accessing or using the Platform you acknowledge that you have read and understood this Privacy Policy and consent to the practices described herein. If you do not agree with this Policy, please do not use our services.

This Policy is designed to meet the requirements of the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and applicable provincial privacy laws in Canada. Because NotaryPro is expanding its services into the United States, we also describe rights afforded under relevant U.S. privacy laws, including the **California Consumer Privacy Act (CCPA)** and its amendments under the California Privacy Rights Act (CPRA). Where these U.S. laws apply, we will honour those rights in addition to the protections under Canadian law.

2. Scope and application

This Policy applies to personal information collected by NotaryPro about all categories of users defined in the General Terms – **Clients**, **Business Account Holders**, **Notary Partners** and **Affiliates or Resellers** – as well as any person who interacts with our Platform or services. It covers:

- use of our Platform to book, schedule or conduct commissioning, identity verification or document witnessing services;
- the generation, storage and export of legal documents using our AI-powered tools or any other Service Supplement;
- participation in affiliate or reseller programs, including referral tracking and commission payments; and
- any other interactions you have with us, including customer support, marketing, surveys, events and cross-border transactions.

This Policy works alongside the Service Supplements. If a Service Supplement contains additional privacy terms (for example, specific provisions about biometric data for identity verification), those terms apply in addition to this Policy. If there is a conflict between this Policy and a Service Supplement, the supplement will govern for the relevant service. For clarity, any reference in this Policy to biometric identifiers, biometric information or biometric elements of Identification Information is intended to align with, and be interpreted consistently with, the definition and treatment of "Biometric Data" in our Biometric Data Policy and Arbitration Agreement.

This Policy does not apply to aggregated or anonymized data that cannot be used to identify an individual, or to information about corporate entities acting in a business capacity.

Artificial Intelligence Use. We use AI and machine learning to deliver, secure and improve our services, including generating document templates, providing automated suggestions, detecting fraud and enhancing user experience. In some cases, our AI systems analyse personal information and transaction data to produce risk scores or recommendations. We may also use the information you provide to train or fine-tune our AI models so that they become more accurate. We do not sell your data for AI training purposes, and we use technical and organizational measures to protect your privacy when training our models. AI tools are offered for your convenience and do not replace professional judgment; you remain responsible for reviewing AI-generated outputs. Please see the General Terms and Acceptable Use Policy for more information on appropriate use of AI-assisted features.

3. Personal information we collect

We collect the following categories of personal information as necessary to provide our Services:

- **Contact Information** – such as your name, mailing address, email address and phone number.
- **Identification Information** – your government-issued ID (e.g., driver's licence, passport) and any biometric information (such as facial images or voiceprints) used during identity verification processes, which constitute "Biometric Data" as described in our Biometric Data Policy and Arbitration Agreement.
- **Appointment and Transaction Information** – details about appointments you schedule (date, time, location), notarial services requested, documents signed or commissioned and transaction history.
- **Payment Information** – limited payment details such as the last four digits of your payment card and transaction identifiers. Full card information is processed by trusted payment processors; we do not store complete card numbers.
- **Service Usage and Technical Information** – IP address, device identifiers, browser type, operating system, user activity logs, interaction data (clicks, pages visited, time spent on our site) and cookies or similar technologies.
- **Document Content** – copies of documents you upload for commissioning or signing and the content generated through our AI document tools. These documents may contain personal or business information about you or third parties.

- **Feedback and Communications** – information you provide when contacting our support team, responding to surveys, providing testimonials or participating in marketing activities.

4. How we collect personal information

We collect personal information through:

1. **Direct interactions** – when you create an account, book an appointment, upload documents, participate in a video call or correspond with us via email, phone or chat.
2. **Automated technologies** – such as cookies, pixel tags, local storage and analytics tools that collect technical and usage information. You can control cookies through your browser settings. See Section 12 for details.
3. **Third-party partners** – including payment processors, identity verification providers, affiliate networks and marketing partners who share information with us as needed to complete transactions or improve services.
4. **Public sources and referrals** – when you are referred by a Business Account Holder or Affiliate partner; we may receive your contact and appointment information from them.

We do not engage in data scraping or purchase personal information from data brokers.

5. How we use personal information

We use your personal information for the following purposes:

- **Provide and manage services** – to schedule and conduct commissioning appointments, facilitate identity verification, generate documents and process payments.
- **Communication** – to send appointment confirmations, service reminders, policy updates and customer support communications. We may contact document recipients on your behalf to facilitate acceptance of signed documents.
- **Legal and regulatory compliance** – to meet our obligations under applicable laws (e.g., verifying the identity of parties to notarial acts, maintaining audit trails) and to cooperate with law enforcement or regulators.
- **Security and fraud prevention** – to detect and prevent fraud, unauthorized access and other security incidents.
- **Analytics and improvement** – to analyze how our services are used, understand user behaviour and improve our Platform's performance, user experience and content.
- **Marketing** – to personalize marketing campaigns, send promotional emails and suggest services. You may opt out of marketing communications at any time.
- **Business operations** – to manage our business relationships, process payments, administer affiliate programs and complete corporate transactions such as mergers or acquisitions.

6. Legal basis and consent

Under Canadian law, we collect, use and disclose personal information with your consent, which may be implied or explicit depending on the sensitivity of the information and the context. You may withdraw your consent at any time, subject to legal or contractual restrictions (see Section 14). Because NotaryPro operates across borders, we also comply with U.S. laws governing electronic signatures, notarization and privacy. Our practices reflect the requirements of the **Electronic Signatures in Global and National Commerce Act (E‑SIGN Act)** and the **Uniform Electronic Transactions Act (UETA)** in jurisdictions where those laws apply. For residents of U.S. states with comprehensive privacy legislation (including but not limited to California, Colorado, Connecticut, Utah and Virginia), we honour your rights under those laws, such as the right to opt out of targeted advertising or profiling. We rely on the following legal bases, which, where we process personal information on behalf of Business Account Holders, operate in conjunction with the roles and obligations set out in our Data Processing Supplement, and, for Biometric Data, are further described in our Biometric Data Policy and Arbitration Agreement:

- **Consent** – for identity verification, marketing and storing copies of documents for your convenience.
- **Performance of a contract** – to fulfill our obligations when providing the Services you request.
- **Legal obligations** – to comply with laws governing commissioners of oaths and notaries, record retention and anti‑money laundering.
- **Legitimate interests** – to improve our services, secure our Platform and communicate with you about similar services.

For residents of California and other U.S. jurisdictions with privacy laws (such as the Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA) and Virginia Consumer Data Protection Act (VCDPA)), we rely on your consent when required and process your data in accordance with those laws. We do not sell personal information and have not shared personal information for monetary consideration in the past 12 months. When U.S. state laws require a separate privacy notice (for example, for California or Virginia residents), we provide an additional notice on our website. We also comply with state laws governing notarial acts and e‑notarization where applicable.

7. Disclosure of personal information

We may disclose your personal information to:

- **Subsidiaries and affiliates** – within the NotaryPro group for the purposes described in this Policy.
- **Service providers** – such as payment processors (e.g., Square, Stripe, PayPal), identity verification vendors, video conferencing providers (e.g., Twilio), email service providers (e.g., SendGrid) and market research firms. These providers are contractually obligated to protect your information and use it only for our purposes, and, where we act as a processor for Business Account Holders, are engaged and

managed in accordance with our Data Processing Supplement. Where these providers handle Biometric Data, their processing is also subject to the restrictions in our Biometric Data Policy and Arbitration Agreement.

- **Business partners** – Business Account Holders or Affiliate partners who referred you to our services; we share only the information necessary to process a transaction or track commissions.
- **Legal and regulatory authorities** – to comply with court orders, laws or legal processes or to respond to lawful requests from governmental or regulatory authorities.
- **Successors** – in the event of a merger, acquisition, restructuring or sale of assets.
- **Other parties with your consent** – for any other purpose disclosed to you at the time of collection or as permitted by law.

8. International data transfers

NotaryPro is headquartered in Canada but uses service providers and data centers in the United States and other countries. Consequently, your personal information may be transferred outside of your province, territory or country of residence, including to the U.S., where different privacy laws may apply. When we transfer information internationally, we implement contractual safeguards and rely on recognized standards to protect your information. By using the Platform you consent to this transfer, processing and storage.

For our U.S. expansion, we endeavour to align our practices with U.S. federal and state privacy laws. For example, we commit to notifying California residents of their rights to access, correct, delete or opt out of the sharing of their personal information (see Section 13). We also comply with state laws concerning notaries and electronic signatures.

9. Security of personal information

We employ administrative, technical and physical safeguards to protect your personal information against unauthorized access, loss or misuse. These measures include:

- **Encryption** – documents and data are encrypted in transit and at rest using industry standards such as TLS for data in transit and AES‑256 for data at rest.
- **Identity and access management** – OAuth 2.0 authentication, multi‑factor verification, role‑based access controls and secure session tokens.
- **Secure infrastructure** – hosting on Microsoft Azure with built‑in firewalls and intrusion detection, and use of trusted digital signing partners like DocuSign and SignNow.
- **Third‑party assessments** – we undertake regular security reviews and work towards compliance with recognized frameworks such as **SOC 2 Type 2** and **NIST SP 800‑53**, and we partner with vendors who meet similar standards.
- **Limited retention** – we store personal documents for a maximum of **90 days** before deleting them unless longer retention is required by law or requested by Business Account Holders.

Despite our efforts, no security measures are perfect. If we identify a security breach that affects your personal information, we will notify you in accordance with applicable law and describe our response. Additional details about our incident response and breach notification practices are set out in our Security Statement and, where we process personal information on behalf of Business Account Holders, in our Data Processing Supplement.

10. Retention of personal information

We retain personal information only for as long as necessary to fulfill the purposes for which it was collected, including to satisfy legal, accounting or reporting requirements. Our typical retention periods are:

- **Client documents and identity data** – stored for 90 days after creation and then securely deleted, unless longer retention is required by law or requested by a Business Account Holder. When we process such information on behalf of Business Account Holders, retention and deletion are further governed by our Data Processing Supplement, and any Biometric Data contained in these records is retained and destroyed in accordance with our Biometric Data Policy and Arbitration Agreement.
- **Account information** – retained for as long as your account remains active and for a reasonable period thereafter to respond to inquiries, resolve disputes or enforce agreements.
- **Analytics data** – anonymized or aggregated and retained for as long as necessary for business analytics purposes.

We may also anonymize personal information so that it no longer identifies you and use it for research or analytics without further notice or consent.

11. Cookies and similar technologies

We use cookies, local storage, pixels and web beacons to improve your experience, analyze site usage and assist with marketing. Cookies may be set by us (first‑party) or by third parties such as analytics providers and marketing partners. Types of cookies include:

- **Strictly necessary cookies** – required for secure login and basic site functionality.
- **Performance and analytics cookies** – used by Microsoft Clarity, Google Analytics and Google Tag Manager to measure site usage and improve performance.
- **Functional cookies** – used by embedded widgets (e.g., Elfsight) to remember preferences.
- **Marketing cookies** – used by TrustPilot and our marketing partners to personalize advertising.

You can manage your cookie preferences through our cookie banner or adjust your browser settings. Blocking some cookies may impact your experience. For information on industry opt‑out tools, see the Digital Advertising Alliance of Canada and the Network Advertising Initiative.

12. Third-party content and links

Our Platform may include links to third-party websites, applications or plug-ins. Clicking those links may allow third parties to collect or share data about you. We do not control these third-party sites and are not responsible for their privacy policies. We encourage you to read the privacy policy of every site you visit.

13. Your rights

Depending on your jurisdiction, you have the following rights:

- **Access** – You can request confirmation of whether we hold personal information about you and request a copy.
- **Correction** – You can request that we correct inaccurate or incomplete personal information.
- **Withdrawal of consent** – You can withdraw your consent at any time for future uses of your personal information.
- **Deletion** – You can request the deletion of your personal information where it is no longer needed, subject to legal obligations.
- **Data portability** – Subject to applicable law, you may request a copy of certain personal information in a structured, commonly used and machine-readable format.
- **Opt-out of marketing** – You may opt out of receiving marketing communications by clicking the "unsubscribe" link in our emails or contacting us directly.

Residents of certain U.S. states (including California, Colorado, Connecticut, Utah and Virginia) have additional rights under their state privacy laws. These rights may include:

- The right to know the categories of personal information collected, sold or shared;
- The right to opt out of the sale of personal information or the processing of personal information for targeted advertising or profiling;
- The right to limit the use of sensitive personal information;
- The right to appeal decisions regarding your privacy requests; and
- The right not to be discriminated against for exercising these rights.

We honour these rights and provide a mechanism to submit U.S. privacy requests via our support email or through a dedicated privacy request portal on our website. If you are a resident of a state with a privacy law not listed above, please contact us to learn about any rights available to you.

To exercise any of your rights, please contact our Privacy Officer using the information below. We may need to verify your identity before responding. Some requests may be refused where permitted by law (e.g., if disclosure would violate another person's privacy).

14. Withdrawal of consent and marketing preferences

Where you have provided consent to our collection, use or disclosure of your personal information, you may withdraw your consent at any time by contacting us. Please note that

withdrawing consent may affect our ability to provide certain Services. You can opt out of marketing emails by clicking “unsubscribe” or contacting us. You can also clear your browser’s local storage to remove saved cart information.

15. Changes to this Privacy Policy

We may update this Policy to reflect changes in our practices, technologies or legal requirements. We will revise the “Last Updated” date and, if the changes are material, provide notice via the Platform or by email. Your continued use of the Platform after the effective date indicates your acceptance of the revised Policy.

16. Contacting us and lodging complaints

If you have questions, comments or requests regarding this Policy, or if you wish to make a complaint about how your personal information has been handled, please contact our Privacy Officer:

Privacy Officer: Robert Onley
Email: legal@notarypro.ca
Mail: NotaryPro Technologies Inc., 2 Simcoe Street South, Suite 300, Oshawa, ON L1H 8C1, Canada

We aim to respond to all privacy inquiries within thirty (30) days. If you are not satisfied with our response, you may lodge a complaint with the **Office of the Privacy Commissioner of Canada**, the **Information and Privacy Commissioner of Ontario** or, for U.S. residents, the relevant state attorney general or other supervisory authority.