

Privacy Policy

Eastern Fingerprint Services

Effective date: July 17, 2026

Eastern Fingerprint Services respects your privacy and recognizes the sensitive nature of the personal information involved in fingerprinting, background screening, identity verification and Commissioner of Oaths services.

This Privacy Policy explains how we collect, use, disclose, protect, retain and dispose of personal information when you use our website, communicate with us, attend an appointment or purchase one of our services.

Eastern Fingerprint Services follows the privacy principles established under Canada's **Personal Information Protection and Electronic Documents Act**, commonly called PIPEDA. These principles include accountability, meaningful consent, limiting collection, appropriate safeguards, openness, access and correction.

1. Scope of this policy

This policy applies to personal information collected through:

- Our website and online forms
- Secure document uploads
- Online, telephone and in-person bookings
- In-office and mobile appointments
- Virtual Commissioner of Oaths appointments
- Fingerprinting and background-screening services
- Email, telephone and other communications
- Payment transactions
- Client portals and secure document-return pages

This policy does not govern the privacy practices of the RCMP, police services, government agencies, courts, screening providers, payment processors or other independent organizations to which information may be submitted.

2. What is personal information?

Personal information is information about an identifiable individual. Depending on the service requested, this may include:

- Name
- Address
- Telephone number and email address
- Date and place of birth
- Gender or other identifying information required by a service provider
- Appointment information
- Government-issued identification information
- Photographs or images of identification
- Fingerprints and biometric information
- Criminal-record-check information
- Employment and education information
- References and employment-verification information
- Driver's abstract information
- Credit-check information
- Immigration or citizenship information
- Affidavits, statutory declarations and supporting documents
- Billing, payment and transaction information
- Communications with our office
- Technical information associated with website use

We treat fingerprints, identification records, criminal-record information, financial information and legal documents as highly sensitive information.

3. Information we collect

Information you provide directly

We may collect information when you:

- Book an appointment

- Complete an application or consent form
- Attend an appointment
- Submit fingerprints
- Present identification
- Upload a document
- Request a background check
- Participate in a virtual appointment
- Make a payment
- Contact us with a question or complaint
- Request access to or correction of your information

Information collected from authorized organizations

With your consent or where otherwise permitted by law, we may receive information from:

- Employers
- Volunteer organizations
- Government agencies
- Police services
- Screening providers
- Educational institutions
- References
- Other organizations authorized by you

Website information

When you visit our website, our website platform and service providers may automatically collect limited technical information, such as:

- Internet Protocol address
- Device and browser type
- Date and time of access

- Pages visited
- Referring website
- General geographic region
- Cookie and analytics information

This information may be used to operate, secure and improve the website.

4. Why we collect and use personal information

We may collect and use personal information to:

- Identify and communicate with clients
- Schedule, confirm and manage appointments
- Confirm eligibility for a requested service
- Verify identity
- Capture and submit fingerprints
- Conduct or facilitate background checks
- Obtain consent and authorization
- Review documents before a Commissioner of Oaths appointment
- Administer oaths, affirmations and statutory declarations
- Return completed documents or results
- Process payments and issue receipts
- Respond to questions, complaints and access requests
- Maintain necessary transaction and business records
- Prevent fraud, misuse and unauthorized access
- Protect clients, employees, systems and property
- Meet legal, regulatory, contractual, accreditation and insurance requirements
- Investigate and respond to privacy or security incidents

We will not collect, use or disclose personal information for a new, unrelated purpose without obtaining additional consent unless permitted or required by law.

PIPEDA generally requires organizations to obtain meaningful consent and limit collection to information needed for an identified, legitimate purpose.

5. Consent

We seek consent appropriate to the sensitivity of the information and the nature of the service.

Consent may be obtained:

- In writing
- Electronically
- Through a consent checkbox
- Verbally during an appointment
- Through an authorized representative
- Through conduct where the purpose is clear and the information is not highly sensitive

Express consent will normally be required for services involving fingerprints, criminal-record information, credit information, employment screening or disclosure of results to another organization.

You may withdraw consent, subject to legal, contractual, operational and service limitations. Withdrawing consent may prevent us from completing a requested service.

6. Fingerprinting and biometric information

Fingerprints are biometric information linked to an individual's physical characteristics. Biometric information requires heightened protection because it is highly sensitive, generally unique and difficult to replace if compromised.

We collect fingerprints only where reasonably necessary for the service requested.

Fingerprint and related identity information may be used to:

- Complete an RCMP-accredited fingerprinting transaction
- Prepare fingerprint forms or cards
- Submit information to the RCMP or another authorized receiving organization
- Confirm the identity associated with a transaction

- Meet accreditation, security and record-keeping requirements

We do not:

- Sell fingerprint information
- Use client fingerprints for marketing
- Use fingerprints for unrelated employee training
- Use fingerprints to track clients
- Retain fingerprint images merely for convenience
- Disclose fingerprints to an unauthorized employer or organization

Fingerprint information is accessible only to personnel authorized to perform or support the requested service.

Fingerprint transactions may be transmitted to the RCMP, police services, government bodies or other organizations authorized to receive them, depending on the service requested.

7. Background checks and screening services

Depending on the service selected, we may collect information required for:

- Criminal record checks
- Vulnerable-sector-related processes where applicable
- International criminal record checks
- Credit checks
- Reference checks
- Employment verification
- Education verification
- Driver's abstracts
- Social-media or other authorized screening services

We may submit the required information to authorized screening providers, police services, government agencies, credit-reporting organizations or other service providers.

Results will be released only to:

- The individual concerned
- An organization authorized by the individual
- A person or organization permitted or required by law to receive them

An employer arranging appointments for several individuals does not automatically receive each person's results unless appropriate authorization has been provided.

8. Commissioner of Oaths services

Documents presented for commissioning may contain sensitive legal, financial, medical, family, immigration or employment information.

We collect and use these documents only as necessary to:

- Review whether the document is eligible for our service
- Arrange the appointment
- Verify identity
- Administer the oath, affirmation or declaration
- Witness the signing
- Complete and return the document
- Maintain necessary transaction records
- Respond to a concern regarding the service

Access to documents is limited to the Commissioner and authorized personnel who require access to provide the requested service.

A Nova Scotia Commissioner of Oaths may administer oaths and receive affidavits, declarations and affirmations within the scope of the Commissioner's appointment. A Commissioner of Oaths does not have the same authority as a notary public to certify documents as true copies unless separately appointed as a notary.

9. Virtual Commissioner of Oaths appointments

Virtual appointments are available only for eligible documents and where the applicable process permits virtual commissioning.

During a virtual appointment, you may be required to:

- Show valid government-issued photo identification

- Confirm your identity
- Confirm that you are physically located in Nova Scotia
- Confirm that you understand the document
- Confirm that you are signing voluntarily
- Sign the document while observed by the Commissioner
- Upload the signed document through a secure method

Government-issued identification is normally visually inspected. We do not ordinarily retain a copy unless there is a specific lawful, contractual or operational need to do so.

Virtual appointments are **not ordinarily recorded**, and screenshots are not ordinarily taken. Where recording became necessary for a particular service, we would inform you and obtain appropriate consent beforehand.

Clients should participate from a private location and advise the Commissioner if another person is present.

10. Identification verification

We request identification only where reasonably necessary to establish identity or complete the requested service.

We may record limited verification information, such as:

- Type of identification presented
- Whether the name and photograph matched
- Whether the identification appeared valid and unexpired
- That identification was examined

We avoid recording complete identification numbers unless required for the service, by the receiving organization or by law.

Canadian privacy guidance recommends identifying individuals only when necessary and limiting authentication information to what is proportionate to the transaction's risks.

11. Secure document uploads and client portals

Clients should use our secure upload system or client portal when submitting:

- Identification

- Fingerprint-related forms
- Consent forms
- Background-check documents
- Affidavits and statutory declarations
- Signed documents
- Other sensitive records

Clients should upload only documents required for the requested service and should remove unnecessary information where possible.

Secure links and client pages may be protected through passwords, access restrictions, expiration controls or other safeguards. Clients are responsible for protecting any password or link sent to them and should not forward it to unauthorized individuals.

12. Email and electronic communication

Ordinary email may not provide the same protection as a secure document portal.

Clients should not send the following through regular email unless specifically instructed:

- Complete payment-card information
- Card security codes
- Banking passwords
- Social Insurance Numbers
- Complete identification documents
- Fingerprint images
- Sensitive background-check results

Where possible, our emails will contain a secure link rather than sensitive information.

By choosing to communicate with us electronically, you acknowledge that electronic communication may carry privacy and security risks.

13. Payments

Payments may be processed by an authorized third-party payment provider.

Eastern Fingerprint Services does not ordinarily receive or store:

- Complete payment-card numbers
- Card security codes
- Online banking passwords

We may retain limited transaction information, including:

- Client name
- Service purchased
- Amount paid
- Payment date
- Transaction or receipt number
- Payment status
- Refund information

Payment providers process information according to their own privacy and security practices.

Clients should not submit card numbers or card security codes through ordinary email, website messages or document-upload forms.

14. When we disclose personal information

We may disclose personal information:

- With your consent
- To complete the service you requested
- To the RCMP or an authorized police service
- To government agencies or courts
- To background-screening providers
- To payment processors
- To website, hosting, security and technology providers
- To professional advisers such as lawyers, accountants or insurers
- To an organization you have authorized to receive results
- To investigate fraud, misuse or security concerns

- Where permitted or required by law
- In connection with a business reorganization, subject to appropriate safeguards

Service providers receive only the information reasonably necessary to perform their functions and are expected to protect it appropriately.

We do not sell or rent personal information.

15. Service providers and storage outside Canada

Some technology, payment, website, communications or screening providers may process or store information outside Nova Scotia or outside Canada.

Information processed in another jurisdiction may be subject to the laws of that jurisdiction and may be accessible to courts, law-enforcement agencies or government authorities in accordance with applicable law.

We select service providers with consideration for the sensitivity of the information involved and use contractual, organizational or technological safeguards where appropriate.

16. Cookies and website technologies

Our website may use cookies and similar technologies to:

- Maintain website functionality
- Remember preferences
- Improve performance
- Understand how visitors use the website
- Detect security threats
- Support appointment or payment features

You may be able to block or delete cookies through your browser. Some website functions may not operate correctly if cookies are disabled.

Where required, visitors will be given choices regarding optional analytics or marketing cookies.

17. Marketing communications

We may send service-related communications concerning:

- Appointments
- Payments
- Document status
- Results
- Security issues
- Changes to a requested service

We will send promotional electronic communications only where permitted by law and with appropriate consent.

You may withdraw consent to marketing communications by using the unsubscribe method provided or by contacting us. Service-related messages may still be sent where necessary to complete a transaction or appointment.

We do not use fingerprint records, background-check results, identification documents or Commissioner of Oaths documents for marketing.

18. Safeguards

We use administrative, physical and technological safeguards appropriate to the sensitivity of the information, which may include:

- Restricted and role-based access
- Unique user accounts
- Password protection
- Multifactor authentication where available
- Encryption and secure transmission
- Locked rooms and storage cabinets
- Controlled access to fingerprinting areas
- Confidentiality requirements
- Staff privacy and security training
- Secure document-upload systems
- Automatic device locking

- Updated security software
- Access and activity logs
- Secure backups
- Secure paper-record transportation
- Cross-cut shredding or approved secure destruction
- Procedures for responding to privacy incidents

No electronic storage or transmission system can be guaranteed completely secure. We regularly review safeguards and adjust them according to the sensitivity of the information and the risks involved.

19. Employee access and confidentiality

Employees and contractors may access personal information only where required to perform their assigned duties.

Accessing client records out of curiosity or for an unauthorized purpose is prohibited.

Personnel handling personal information are expected to:

- Follow confidentiality requirements
- Use company-approved accounts and devices
- Protect passwords and access credentials
- Avoid discussing client information in public areas
- Report suspected privacy incidents immediately
- Return or securely destroy records when instructed

Access is removed when it is no longer required or when employment or contractual duties end.

20. Mobile appointments

During mobile fingerprinting or other off-site services, we take steps to protect client information, including:

- Using company-authorized equipment
- Keeping documents and equipment under staff control

- Transporting paper documents in secure containers
- Limiting information taken to the appointment
- Conducting appointments in an appropriately private area
- Avoiding discussions where unauthorized people can hear
- Securely uploading records
- Removing temporary local files when no longer required
- Returning documents to the secure office promptly

Clients and employers arranging mobile appointments are expected to provide an area that allows reasonable privacy.

21. Retention and secure destruction

We retain personal information only for as long as reasonably necessary to:

- Complete the requested service
- Deliver documents or results
- Respond to client questions
- Meet legal, regulatory or contractual requirements
- Meet RCMP, screening-provider or accreditation requirements
- Maintain accounting and tax records
- Resolve disputes or complaints
- Protect against fraud or legal claims

Different records may have different retention periods.

Uploaded documents, identification images, fingerprint transaction records, screening records, payment records and Commissioner of Oaths records may therefore be retained for different lengths of time.

When information is no longer required, it is securely deleted, anonymized or destroyed using methods appropriate to its format and sensitivity.

22. Accuracy

We take reasonable steps to keep personal information accurate, complete and up to date for the purposes for which it is used.

Clients are responsible for providing accurate information and informing us promptly of errors or changes.

Where information has already been submitted to the RCMP, another government agency or a screening provider, correction may be subject to that organization's procedures.

23. Accessing your information

Subject to legal exceptions, you may request:

- Confirmation of whether we hold personal information about you
- Access to that information
- An explanation of how it has been used
- Information about organizations to which it has been disclosed
- Correction of inaccurate or incomplete information

We may ask you to provide information sufficient to verify your identity before responding.

Access may be limited where disclosure would:

- Reveal another person's personal information
- Reveal confidential commercial information
- Be prohibited by law
- Interfere with a legal proceeding or investigation
- Create a serious risk to another person
- Involve information we are not legally permitted to release

Where we cannot provide access, we will explain the reason where legally permitted.

24. Privacy complaints and concerns

Questions, access requests and complaints should be directed to our Privacy Officer.

We will:

- Acknowledge the concern
- Review the circumstances

- Request additional information where necessary
- Take corrective action where appropriate
- Explain the outcome of our review

You may also have the right to contact the Office of the Privacy Commissioner of Canada.

25. Privacy breaches

A privacy breach may include unauthorized access, use, loss, disclosure, alteration or destruction of personal information.

Examples include:

- Sending a document to the wrong person
- Lost paperwork or equipment
- Unauthorized employee access
- Compromised passwords
- Malware or ransomware
- Exposure of a secure upload
- Results placed in the wrong client portal

Where a breach occurs, we will take reasonable steps to:

1. Contain the incident.
2. Investigate what happened.
3. Determine what information was affected.
4. Assess the potential risk to individuals.
5. Notify affected individuals where appropriate or required.
6. Notify regulators or other organizations where legally required.
7. Maintain required breach records.
8. Take steps to reduce the risk of recurrence.

Under PIPEDA, organizations have reporting, notification and record-keeping obligations for breaches that create a real risk of significant harm.

26. Children and minors

Some services may be provided to minors where legally permitted and appropriate.

Depending on the circumstances, we may require the involvement or consent of a parent, guardian or authorized representative.

We will collect only the information necessary to complete the service and will apply safeguards appropriate to the sensitivity of the information and the age of the individual.

27. Third-party websites

Our website may contain links to third-party websites.

Eastern Fingerprint Services is not responsible for the privacy, security, availability or content of websites operated by other organizations. Clients should review the privacy policies of those organizations before providing personal information.

28. Changes to this policy

We may update this Privacy Policy to reflect:

- Changes to our services
- Changes to legal or regulatory requirements
- New technology
- Changes to service providers
- Improvements to our privacy practices

The current version will be posted on our website with its effective date.

Material changes may also be communicated through the website, email or another appropriate method.

29. Contact our Privacy Officer

Questions, complaints, access requests and correction requests may be directed to:

Privacy Officer

Eastern Fingerprint Services

25 Raddall Avenue, Unit 1
Dartmouth, Nova Scotia B3B 1L4

Telephone: 902-468-3456

Email: info@easternfingerprints.ca

Website: www.easternfingerprints.ca