DATA PROTECTION

Canada Privacy Notice

How we use and protect your personal information

FCL PN CA 001 | Version 1.0

15 November 2026

Final

Finaffairs Consulting Inc

compliance@finaffairsconsulting.com

1 Who we are and what we collect

Finaffairs Consulting Inc is responsible for the personal information it collects and uses for its own purposes in connection with its Canadian operations.

The Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial laws govern our handling of personal information. PIPEDA excludes business contact details used solely to communicate with someone about their work, business or profession.

Who this notice covers

This notice covers website visitors, prospective and existing clients, client personnel and research participants, suppliers and partners, job applicants and independent consultants, and Academy learners and event attendees. Staff receive separate workforce privacy information. A recruitment process, research project or other activity may provide additional information when it collects your data.

When we handle personal information only on a client's documented instructions, the client generally determines why and how it is used. Contact the client to exercise your rights over that information. We will help the client respond where appropriate. We are responsible for information we use for our own purposes, such as business administration and responding to enquiries.

What we collect

Contact and professional details. Name, work and personal contact details where relevant, employer, role, professional profile, and correspondence.

Services and transactions. Enquiries, proposals, contracts, invoices, project records and bank details needed to pay consultants and suppliers.

Recruitment and learning. CVs, work history, qualifications, references, registrations, attendance, assessment results and feedback.

Website and device information. Technical information needed to deliver and secure the website, such as IP addresses, device and browser details, and security logs.

Work eligibility and equality monitoring. Identity or work-eligibility documents where Canadian employment or immigration rules require them. Voluntary employment equity data may include information on disability or racial or ethnic identity.

Events and meetings. Dietary and accessibility needs, including health information such as allergies or disability-related adjustments, and photos, video or audio recordings from events, webinars or Microsoft Teams meetings where recorded.

Research. Research participants may disclose sensitive personal information in interviews or surveys, such as health information, ethnicity or beliefs.

2 How we use and share information

Where the information comes from

Information comes from you, your device or, where relevant, an employer, client, partner, referee, recruitment or verification provider, or public sources such as company registers and professional profiles.

How we use personal information

Enquiries and engagement delivery. Respond to requests, prepare proposals, administer contracts, deliver consulting, research, Academy programmes and events, and communicate with participants.

People and supplier management. Evaluate applicants and independent consultants, arrange interviews and checks where relevant, manage suppliers and procurement, and process billing and payments.

Communications and improvement. Send permitted updates, record preferences and review feedback to improve our services.

Security and accountability. Protect accounts and systems, investigate misuse, manage conflicts and risks, keep necessary records, resolve disputes and meet legal obligations.

Consent and choices

We obtain meaningful consent where required. Depending on the purpose, sensitivity and reasonable expectations, consent may be express or implied. We generally ask for express consent for sensitive information or when the use falls outside reasonable expectations. We explain significant new purposes and seek fresh consent where required. We may use statutory exceptions where the law authorizes collection, use or disclosure without consent.

You can withdraw consent, subject to legal or contractual restrictions and reasonable notice. We explain what withdrawal means for the service. We collect information needed for the identified purpose. If you choose not to provide essential information, we may be unable to complete the relevant service or application.

Who receives information

Providers and delivery partners. Hosting, email, collaboration, learning, event, recruitment and IT providers may handle information to support the service. Approved specialists and delivery partners may receive information needed for the work.

Clients and sponsors. Where relevant to the engagement or programme, client contacts or training sponsors may receive agreed outputs, attendance, completion or assessment information. We tell you about project-specific disclosures where required.

Business and legal recipients. Relevant Finaffairs offices, banks and payment providers, auditors, insurers and advisers may receive information for administration or delivery. Regulators, courts and public authorities may receive information where permitted or required. A party involved in a proposed business transaction may receive limited information subject to appropriate safeguards.

3 Transfers and privacy preferences

Processing inside and outside Canada

Finaffairs offices and providers in Canada or abroad may handle information for activities such as hosting, IT support, communications and engagement delivery. We remain accountable for information transferred to a provider for processing and use contractual or other measures to provide comparable protection, as required. Courts, regulators or law enforcement in another country may have lawful access under that country's laws. Contact our privacy contact for information about providers outside Canada and the policies that govern their use.

Where Québec's private sector privacy law applies, we assess privacy risks before communicating information outside Québec and use a written agreement and adequate safeguards as required.

How we protect information

We use administrative, technical and physical safeguards appropriate to the sensitivity and risk of the information, including access controls and measures to protect information handled by providers. If an incident triggers a legal notification requirement, we notify affected people and authorities as required.

Website cookies and tracking

Our website does not use analytics, advertising or tracking cookies, and does not allow third parties to collect information about your browsing over time or across other websites. Because we do not track visitors, our website does not change its behaviour in response to Do Not Track or Global Privacy Control signals.

Commercial electronic messages

We send commercial electronic messages with the consent or other authority required by Canada's anti-spam legislation (CASL). Use the unsubscribe link or contact us. For messages subject to CASL's unsubscribe requirement, we act without delay and within 10 business days.

Automated decisions and sensitive information

When an applicable law requires notice of a decision based exclusively on automated processing, we explain the decision and how you can ask about the information used, the main reasons and factors, and how to request correction or submit observations for review. We explain sensitive collection at the point of collection, including accommodation requests and sensitive research disclosures. Where we solicit voluntary demographic information or intend to record an event, webinar or Teams meeting, we explain its intended use and applicable choices.

4 How long we keep your information

The periods below apply to records we keep for our own purposes. For personal information we handle on a client's instructions, the engagement terms and applicable law govern retention and return or deletion.

Record type	Retention period or criteria
Unsuccessful applicants	6 months after the recruitment decision. If provincial law requires a longer period, that period applies. For example, British Columbia generally requires at least 1 year for information used in a decision directly affecting an individual.
Financial and tax records	Generally 6 years from the end of the last tax year to which the records relate, subject to CRA exceptions.
Client contracts	Contract term plus 6 years after it ends.
Academy records	6 years after course completion or withdrawal.
Marketing records	Until you opt out or our authority to send messages under CASL ends, whichever is earlier.
Enquiries without an engagement	2 years from our last contact.
Supplier records	Duration of the relationship plus 6 years after it ends.
Website security logs	12 months from creation.
Work eligibility records	For as long as needed to demonstrate work eligibility or comply with a recordkeeping requirement tied to the relevant work permit or employer programme.
Consultant bank details	Until final payment and reconciliation. Payment evidence follows the financial and tax period.
Equality and event support records	Until monitoring results are compiled or event support and related follow-up are complete. We keep identifiable records longer only where required by law or necessary to resolve a claim.
Recordings and research data	For the period stated at collection or until the stated use ends. For research, this includes analysis and validation of findings. Client instructions apply where we act for a client.

Legal, regulatory or contractual obligations, audits, complaints and litigation holds may require longer retention. After the applicable period we securely delete or anonymise the information. We keep a limited suppression record to honour marketing opt-outs.

5 Your rights and how to contact us

Access correction and complaints

You can request access to your personal information and information about how it has been used and disclosed. You can challenge the accuracy or completeness of your information and ask for correction, and challenge our compliance. We normally respond to a written access request under PIPEDA within 30 days, subject to lawful extensions. Additional rights, including portability or cessation of dissemination in some circumstances, may apply under provincial law.

Privacy Office | compliance@finaffairsconsulting.com
Finaffairs Consulting Inc, 2 Bloor Street West, Suite 700, Toronto, ON M4W 3E2, Canada

Describe the request and the service or interaction it concerns. We may ask for information needed to verify your identity or a representative's authority. Please wait for secure submission instructions before sending identity documents or other sensitive information.

If your concern remains unresolved, you may contact the Office of the Privacy Commissioner of Canada or the applicable provincial regulator, such as the Commission d'accès à l'information du Québec, depending on which law applies.

Changes to this notice

We post the latest version on the relevant website and notify affected people of material changes where the law requires. The cover shows the date of this version.

Regulator and legal information

Office of the Privacy Commissioner • Québec private sector privacy law • CRTC guidance on CASL

Version history

Document control	Release information
Reference and version	FCL PN CA 001 | Version 1.0 | Final
Release date and summary	15 November 2026 | First final issue of this jurisdiction's notice.