DATA PROTECTION

United States Privacy Notice

How we use and protect your personal information

FCL PN US 001 | Version 1.0

November 15, 2026

Final

Finaffairs Consulting Inc

compliance@finaffairsconsulting.com

1 Who we are and what we collect

Finaffairs Consulting Inc is responsible for personal information it collects and uses for its own purposes in connection with its U.S. operations. This notice explains those practices and how you can exercise your privacy rights.

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 and work-authorization documents for Form I-9 where required. Voluntary equal employment opportunity information may include race, ethnicity, disability or veteran status, where applicable.

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 information in interviews or surveys, such as health, race or ethnicity, or religious beliefs.

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.

2 How we use and share information

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.

Sensitive information

We use work-authorization records for employment verification where required and consultant bank details to make payments. We use accommodation information to arrange access and voluntary demographic information for lawful equal opportunity monitoring or reporting. We explain how we handle sensitive research information and event or Teams recordings when we collect them, and seek authorization or consent where required. A separate authorization and required disclosures apply if we obtain a consumer report for employment purposes under the Fair Credit Reporting Act.

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.

Where information is handled

We or our service providers may store or access information in the United States and other countries where we operate or obtain services. Information in those countries may be subject to local law and lawful requests by authorities.

3 Website and state privacy choices

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.

State privacy rights

Depending on where you live, the law's coverage and the type of information, you may have rights to confirm processing, access information, correct inaccuracies, request deletion and obtain a portable copy. Some state laws also give you rights to information about recipients, to opt out of sale, sharing for cross-context behavioral advertising, targeted advertising or certain profiling, or to limit certain uses or disclosures of sensitive personal information. We honor applicable rights and prohibit unlawful discrimination or retaliation for exercising them.

Making and appealing a request

Use the contact details under Requests and contact details. Where permitted, an authorized agent may act for you. We may verify your identity or the agent's authority when the law allows. We respond within the applicable law's time limits and explain permitted extensions or denials. Where a right of appeal applies, email us with the subject "Privacy appeal" and the original case details. We explain the result and how to contact the relevant state authority where required.

Marketing and children

Use the unsubscribe link in our commercial emails or contact us to stop receiving them. Service messages may still be sent. Our general business websites and professional services are intended for adults. If you believe a child under 13 provided personal information online, contact us so we can investigate and take the steps required by law.

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 where permitted. Covered EEOC records are kept at least 1 year from record creation or the personnel action, whichever is later. Where California Government Code §12946 applies, covered records are kept at least 4 years.
Financial and tax records	6 years from the end of the relevant tax year, subject to longer federal or state requirements.
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 we stop using the contact for marketing.
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 Form I-9 and retained supporting documents, 3 years from hire or 1 year after employment ends, whichever is later.
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 anonymize the information. We keep a limited suppression record to honor marketing opt-outs.

5 Requests and contact details

Contact us about privacy

Privacy Contact | compliance@finaffairsconsulting.com
Finaffairs Consulting Inc, One Pierrepont Plaza, 300 Cadman Plaza West, 12th Floor, Brooklyn, NY 11201, United States

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.

You may also raise a concern with your state attorney general or the relevant state privacy authority. California residents can contact the California Privacy Protection Agency where applicable.

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.

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

California privacy laws and regulations • New York SHIELD Act • FTC consumer reporting

Version history

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