FINAFFAIRS CONSULTING LTD.

DATA PROTECTION

United Kingdom Privacy Notice

How we use and protect your personal information

FCL PN UK 001 | Version 1.0

15 November 2026

Final

Finaffairs Consulting Ltd

UK company number 08324763

compliance@finaffairsconsulting.com

1 Who we are and what we collect

Finaffairs Consulting Ltd (company number 08324763) is the controller for the activities covered by this notice where it decides why and how personal information is used. This notice explains our practices under the UK GDPR and Data Protection Act 2018, as amended, and the Privacy and Electronic Communications Regulations (PECR).

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 documents and check records for UK right-to-work verification where required. Equality monitoring may include ethnicity, disability or other special category data.

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 special category data in interviews, surveys or workshops, including health, ethnicity, beliefs or political opinions.

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 Why we use your information

We use personal information for the purposes below. The legal basis depends on what we do and your relationship with us.

Enquiries and contracts. We respond to enquiries, take requested steps before entering a contract with you and deliver our obligations under that contract. For corporate client contacts, proposals and relationship management, we rely on legitimate interests in operating our business and delivering the engagement.

Consulting, research and learning. We deliver projects, workshops, events and Academy training, manage participation and evaluate delivery. We rely on contract where we provide a service under a contract with you and on legitimate interests in delivering, evaluating and improving services in other cases. We seek consent where a specific optional activity requires it.

Recruitment and procurement. We assess suitability, contact referees where appropriate and manage applications, suppliers and tender submissions. We rely on requested pre-contract steps where applicable, legitimate interests in selecting suitable people and suppliers, and legal obligation for checks the law requires.

Administration, security and compliance. We rely on legal obligation for statutory accounting, reporting or disclosures. We rely on legitimate interests to administer business relationships, prevent fraud, protect systems, manage conflicts and pursue or defend claims.

Marketing and website operation. We rely on consent where required and on legitimate interests where permitted to promote our services and operate and secure our website. We apply the separate rules for electronic marketing and storing or accessing information on your device.

Sensitive information and criminal records

If we collect health information for accessibility arrangements or other special category data through equality monitoring or research, we identify both an Article 6 basis and a separate Article 9 condition, such as explicit consent where appropriate or an applicable employment, equality monitoring, research or legal claims condition. Where the Data Protection Act 2018 requires it, we also apply the relevant Schedule 1 condition and safeguards. For criminal offence data, we identify a lawful basis and the additional authority required by Article 10 and the Data Protection Act 2018. We explain the relevant processing at the point of collection.

When we need you to provide information

We identify required fields or explain when a law or contract requires information. If you withhold details needed to fulfil a request or meet an obligation, we may be unable to provide the service, process an application or complete the relevant transaction.

3 Sharing and protecting data

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.

Transfers outside the United Kingdom

Depending on the service or engagement, personal information may be hosted or accessed overseas by other Finaffairs offices or by service providers. For a restricted transfer, we rely on applicable UK adequacy regulations or on a lawful safeguard, such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, together with a transfer assessment where required. We use statutory exceptions only where their conditions are met. Contact us for the destinations relevant to your information or a copy of the applicable safeguard.

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.

Photography and recording

We tell you when an event, webinar or Teams meeting will be photographed or recorded and explain the purpose and intended audience. We seek consent where required and explain any options for participating without appearing in a recording.

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.

Electronic marketing

You can unsubscribe from electronic marketing using the message link or by contacting us. We will stop using your information for direct marketing if you object.

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.
Financial and tax records	6 years from the end of the relevant accounting period, or longer if required by HMRC rules.
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, withdraw consent or the basis for marketing ends.
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 required right-to-work checks, throughout employment and for 2 years after employment ends.
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

Your data protection rights

You can ask for access to your personal information, correction of inaccurate information, erasure, restriction or portability where the relevant conditions apply. You can object to processing based on legitimate interests and object at any time to direct marketing, including related profiling. You can withdraw consent at any time. Withdrawal leaves earlier lawful processing unaffected.

Automated decisions

If we use solely automated processing to make a decision that produces a legal or similarly significant effect, we will explain the decision, the logic involved and what it means for you. Where the applicable rules require safeguards, you can make representations, obtain human intervention and contest the decision.

Make a request or complaint

Privacy Contact | compliance@finaffairsconsulting.com
Finaffairs Consulting Ltd, 5 Brayford Square, London E1 0SG, United Kingdom

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.

We normally respond to rights requests within one month, subject to lawful extensions or adjustments. We acknowledge data protection complaints within 30 days, take appropriate steps to investigate, keep you informed and communicate the outcome without undue delay. You can also complain to the Information Commission (ICO).

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

ICO complaints • ICO guidance on privacy information • ICO guidance on handling complaints

Version history

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