FINAFFAIRS CONSULTING LTD.

DATA PROTECTION

Nigeria Privacy Notice

How we use and protect your personal information

FCL PN NG 001 | Version 1.0

15 November 2026

Final

Finaffairs Consulting Ltd

compliance@finaffairsconsulting.com

1 Who we are and what we collect

Finaffairs Consulting Ltd is the controller when it determines why and how to process personal data in connection with its Nigerian operations. This notice explains how we handle that data under the Nigeria Data Protection Act 2023 and the General Application and Implementation Directive 2025.

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-authorisation documents where required under Nigerian employment or immigration rules. Equality monitoring may include demographic information and disability where relevant.

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 data in interviews, surveys or workshops, such as health status, ethnic origin, 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 Purposes and lawful bases

Enquiries and services. We take requested steps before a contract with you or perform our obligations to you under a contract. We rely on legitimate interests in responding to corporate enquiries and delivering or evaluating client engagements, training and events where those interests are lawful and do not override your rights.

Recruitment and procurement. We assess applications and suppliers and manage proposals based on requested pre-contract steps where applicable and our legitimate interests in evaluating suitability. We rely on a legal obligation when a check or record is required by law.

Records risk and compliance. We rely on legal obligations for statutory recordkeeping, reporting and lawful disclosures. We rely on legitimate interests in information security, preventing misuse, managing conflicts and resolving disputes, subject to the required balancing assessment.

Marketing and optional activities. We seek consent when required for promotional communications or optional activities such as recording or publicity. Where permitted, we may rely on a documented legitimate interest for other activities, subject to your rights. You can withdraw consent or object to marketing at any time.

How we process data

We may use paper and electronic records, secure communications, interviews, online forms, client and learning platforms, and business systems. Depending on the engagement, staff or authorised providers may review records, verify relevant details and analyse responses or participation. We explain activity-specific uses when we collect the information where required.

Sensitive data and children

For sensitive data, including health information in accommodation requests, applicable equality monitoring information and sensitive interview disclosures, we identify a lawful basis and an applicable condition under section 30 of the Act, such as valid consent or necessity for legal claims. We restrict access to sensitive information. For event or Teams recordings, we tell participants the purpose, intended recipients and available choices before recording. If a service involves a child or a person who lacks legal capacity and we rely on consent, we obtain and verify the parent or legal guardian's consent where the Act requires it.

When we need you to provide data

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.

Marketing choices

Use the unsubscribe link or contact us to object to direct marketing, including related profiling. We stop processing your data for direct marketing once you object.

3 Sharing and protecting data

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.

Who receives data and why

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 Nigeria

Personal data may be transferred to, stored in or remotely accessed from other countries where Finaffairs offices or providers support an engagement or service. We apply sections 41 and 42 of the Act. We document the transfer basis and use a mechanism giving an adequate level of protection, such as applicable law, approved contractual safeguards or another recognised mechanism. Where adequate protection is unavailable, we transfer only if a statutory exception applies and its conditions are met. Ask us about destinations and safeguards relevant to your data.

How we protect data

We apply safeguards appropriate to the data and risk. If a breach is likely to pose a risk to people's rights and freedoms, we notify the Nigeria Data Protection Commission (NDPC) within 72 hours of becoming aware of it as required. Where the breach is likely to result in a high risk, we immediately inform affected people in accordance with the Act.

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	At least 6 years after the year of assessment to which the records relate, as required by the Nigeria Tax Administration Act 2025.
Client contracts	Contract term plus 6 years after it ends.
Academy records	6 years after course completion or withdrawal.
Marketing records	Until you object, 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 as long as needed to demonstrate eligibility or comply with recordkeeping requirements tied to the relevant employment or immigration authorisation.
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 whether we hold your data and obtain access and a copy. Depending on the circumstances, you can request correction, erasure, restriction or portability. You may withdraw consent at any time. You can object to processing and ask us to stop processing for direct marketing, including related profiling. We apply the conditions and exceptions in the Act.

Automated decisions

You generally have the right to avoid decisions based solely on automated processing, including profiling, that have legal or similarly significant effects. If a lawful exception applies and we carry out such processing, we explain its significance and expected consequences. We provide applicable safeguards such as human intervention, the opportunity to express your view and a way to challenge the decision.

Requests and complaints

Data Protection Contact | compliance@finaffairsconsulting.com
Finaffairs Consulting Ltd, Nigeria Office, 2nd Floor, Cube Ameen Plaza, Plot 1782 Adetokunbo Ademola Crescent, Wuse 2, Abuja, FCT, Nigeria

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 can raise a concern directly with us or lodge a complaint with the NDPC under section 46 of the Act. You may use the Commission's standard grievance notice for internal remediation.

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

Nigeria Data Protection Commission • Nigeria Data Protection Act 2023 • Implementation Directive 2025

Version history

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