

Privacy Policy

How we collect, use and protect your Personal Data Issued under the Data Protection Act, 2019 (Kenya)

Field	Detail	Field	Detail
Version	1.0	Effective Date	1 January 2026
Owner	Board of Directors	Next Review	1 January 2027
Approved By	Board of Directors	Approval Authority	Board Chairman
Contact	info@entropy.ke	Jurisdiction	Republic of Kenya

1. Introduction

Entropy Africa Industries Ltd (“Entropy”, “we”, “us”, “our”) is a professional services firm headquartered in Nairobi, Kenya, that connects African professionals with global organisations expanding into Africa. We take the protection of your Personal Data seriously and are committed to processing it lawfully, fairly and transparently in accordance with the Data Protection Act, 2019, the Data Protection (General) Regulations, 2021 and applicable international standards.

This Privacy Policy explains who we are, what Personal Data we collect, why we collect it, how we use and share it, how long we keep it, where it is stored, and what rights you have. It applies to:

- visitors to our website at www.entropy.ke and any digital properties we operate;
- prospective and current clients and their representatives;
- job applicants, candidates and placed talent engaged through our Global Team Infrastructure pillar;
- our consultants, contractors and suppliers; and
- any other natural person whose Personal Data we process.

By using our services or our website, you confirm that you have read this Privacy Policy. Where the law requires your Consent for specific processing, we will ask for it separately.

2. Who We Are and How to Contact Us

Entropy Africa Industries Ltd is a company incorporated in Kenya. For any matter relating to this Privacy Policy or to your Personal Data, please contact us at:

- Email: info@entropy.ke
- Website: www.entropy.ke

Entropy is committed to registering with the Office of the Data Protection Commissioner (ODPC) as a Data Controller and Data Processor under the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021. Pending issuance of the registration certificate, we operate in full substantive compliance with the Data Protection Act, 2019.

3. Personal Data We Collect

We collect Personal Data in the following ways:

3.1 Information you give us

This may include your name, contact details (email, phone, postal address), national identification or passport details, KRA Personal Identification Number (PIN), date of birth, professional and employment history, qualifications

and references, project details you share with us, payment information and any other information you choose to provide through our website, application forms, in person, by email, by telephone or through a service provider.

3.2 Information we collect automatically

When you visit our website, we automatically collect certain information about your device and visit, including IP address, browser type, operating system, referring URL, pages visited and time spent. This is collected through cookies and similar technologies (see Section 9).

3.3 Information from other sources

Where lawful and necessary, we may receive Personal Data about you from third parties, including referees you nominate, identity verification and KYC providers, professional networks (e.g., LinkedIn), publicly available registers, regulators, our clients (where you are a candidate or placed-talent referred by them), and our service providers.

3.4 Sensitive Personal Data

We process Sensitive Personal Data (as defined in the Data Protection Act) only where necessary, on a specific lawful basis under Section 44 of the Data Protection Act and with heightened safeguards. Examples include health information where required for workplace accommodation, or biometric data where used for office access.

4. How We Use Your Personal Data and Lawful Bases

We process your Personal Data only where one or more of the following lawful bases under Section 30 of the Data Protection Act applies. The table below explains, for each main purpose, the data we use and the lawful basis.

Purpose	Data Used	Lawful Basis
Delivering consulting services and managing client relationships	Identity, contact, engagement, financial data	Performance of a contract; legitimate interests
Sourcing, vetting and placing talent for clients	Identity, professional history, references, KYC, sensitive data where relevant	Performance of a contract; Consent for non-essential data
KYC, AML, sanctions screening and fraud prevention	Identity, ID/PIN, beneficial ownership, screening results	Legal obligation; legitimate interests
Invoicing, payments and accounting	Identity, contact, payment, tax data	Performance of a contract; legal obligation
Statutory, regulatory and tax reporting	Identity, financial, employment data	Legal obligation
Communicating with you (updates, responses, service messages)	Identity, contact data	Performance of a contract; legitimate interests
Marketing and industry insights	Contact data, communication preferences	Consent (or legitimate interests for existing contacts, with opt-out)
Website operation, security and analytics	Device data, IP address, cookies	Legitimate interests; Consent for non-essential cookies

Purpose	Data Used	Lawful Basis
Recruitment of our own personnel	CV, references, qualifications	Steps prior to entering into a contract; Consent
Improving our services and developing new offerings	Aggregated and pseudonymised data	Legitimate interests
Establishing, exercising or defending legal claims	Any relevant data	Legitimate interests; legal obligation

5. Who We Share Your Personal Data With

Entropy does not sell your Personal Data. We share Personal Data only where necessary and only with the following categories of recipient, under written confidentiality and, where applicable, data processing agreements:

- **Our clients and prospective clients:** where you are a candidate, placed talent, consultant or counterparty in an engagement we deliver.
- **Our service providers:** including cloud and IT hosting providers, communication platforms, accounting and payroll providers, KYC and identity verification providers, and AI tools we use to deliver services.
- **Professional advisers:** including lawyers, auditors, insurers and consultants providing services to Entropy.
- **Public authorities and regulators:** including the Kenya Revenue Authority, the ODPC, courts and other competent authorities where legally required.
- **Counterparties and their representatives:** in connection with transactions, due diligence or contracts in which you are involved.
- **Successors in interest:** in connection with a corporate transaction, where any successor is bound by terms no less protective than this Policy.

6. International Transfers of Personal Data

Because we serve international clients and engage international service providers, your Personal Data may be transferred to, stored in, or accessed from jurisdictions outside Kenya. Whenever we transfer Personal Data outside Kenya, we do so only where one of the conditions in Sections 48 and 49 of the Data Protection Act is met, including:

- a finding by the ODPC that the recipient jurisdiction provides an adequate level of protection;
- appropriate safeguards such as standard contractual clauses approved by the ODPC or equivalent contractual protections;
- necessity for the performance of a contract with you, or for pre-contractual steps at your request;
- necessity for the performance of a contract concluded in your interest;
- important public interest reasons, or the establishment, exercise or defence of legal claims;
- the protection of your vital interests; or
- your explicit Consent after being informed of the risks.

Transfers of Sensitive Personal Data outside Kenya are made only where explicit Consent or another high-bar ground under Section 49 of the Data Protection Act applies. A summary of our cross-border transfer mechanisms is available on request from info@entropy.ke.

7. How Long We Keep Your Personal Data

We keep your Personal Data only as long as is necessary for the purpose for which it was collected, including for the purposes of satisfying any legal, accounting, regulatory or reporting requirements, or the establishment, exercise or

defence of legal claims. The category-by-category retention periods that govern our practices are summarised below; specific periods are recorded in our internal Retention Schedule.

Category	Examples	Retention
Client engagement records	Engagement letters, deliverables, correspondence	7 years from end of engagement
KYC / AML records	ID, PIN, beneficial ownership, screening	7 years from end of relationship
Candidate / talent records (placed)	CV, references, placement contract	7 years from end of placement
Candidate records (not placed)	CV, application data, interview notes	24 months from last contact
Financial and tax records	Invoices, receipts, ledgers, filings	7 years
Marketing contact data	Email list under Consent	Until Consent withdrawn or 3 years of inactivity
Website analytics	IP, cookies, session data	13 months

At the end of the retention period, we securely delete or irreversibly anonymise your Personal Data.

8. How We Protect Your Personal Data

We have implemented appropriate technical and organisational measures to protect your Personal Data against accidental or unlawful loss, alteration, unauthorised disclosure or access, including:

- role-based access controls and the principle of least privilege;
- multi-factor authentication on systems holding Personal Data;
- encryption of Personal Data in transit and, where reasonable, at rest;
- secure configuration, patching and monitoring of our endpoints, servers and SaaS applications;
- written confidentiality obligations on all personnel and contractors;
- vendor due diligence and data processing agreements with our service providers;
- regular data protection and information security training; and
- documented incident detection and response procedures.

No method of transmission over the internet or method of electronic storage is completely secure. While we use commercially reasonable means to protect your Personal Data, we cannot guarantee its absolute security.

9. Cookies and Similar Technologies

Our website uses cookies and similar technologies to operate the site, remember your preferences, understand how visitors use the site and improve your experience. We use the following categories:

Category	Purpose	Basis
Strictly necessary	Site functioning, security, load balancing, session management	Necessary — no Consent required

Category	Purpose	Basis
Functional	Remembering your preferences, language settings, form data	Consent
Analytics / performance	Understanding usage, page popularity, debugging, improvement	Consent
Marketing	Measuring campaign effectiveness; not used for cross-site targeting unless disclosed	Consent

Where the law requires your Consent for non-essential cookies, we obtain that Consent through our cookie banner before such cookies are set. You can withdraw your Consent at any time through the cookie settings link in the footer of our website or via your browser settings. Refusing non-essential cookies will not prevent you from using the website but may limit some functionality.

10. Automated Decision-Making, Profiling and AI

Entropy operates an AI-Enabled Business Process Outsourcing pillar and uses AI and analytical tools to deliver services. We do not subject you to a decision based solely on automated processing (including profiling) that produces legal or similarly significant effects on you, except as expressly permitted by Section 35 of the Data Protection Act. Where AI is used in a way that materially affects you, you will be informed and, where applicable, given the opportunity to request human review.

11. Your Rights

You have the following rights in relation to your Personal Data, subject to the exemptions and limitations in the Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021:

- **Right to be informed** about how your Personal Data is used.
- **Right of access** to a copy of the Personal Data we hold about you.
- **Right to rectification** of inaccurate, incomplete, out-of-date or misleading data.
- **Right to erasure** in the circumstances set out in Section 40 of the Data Protection Act and Regulation 13 of the Data Protection (General) Regulations, 2021.
- **Right to restrict processing** in defined circumstances.
- **Right to data portability** where technically feasible.
- **Right to object** to processing on grounds relating to your particular situation, including direct marketing.
- **Right to withdraw Consent** at any time, without affecting the lawfulness of pre-withdrawal processing.
- **Right not to be subject to a solely automated decision** with legal or similarly significant effects.
- **Right to lodge a complaint** with the ODPC.

How to exercise your rights

Please send your request to info@entropy.ke. We may need to verify your identity using reasonable means proportionate to the sensitivity of the data. We will acknowledge your request within 7 calendar days and substantively respond within 30 calendar days, extendable by a further 30 days for complex requests with notice to you. We do not charge a fee unless your request is manifestly unfounded or excessive, in which case we will tell you and explain why.

If we refuse a request in whole or in part, we will provide our reasons in writing and inform you of your right to internal review and of your right to complain to the ODPC.

12. If You Apply for a Role Through Us

If you apply to join Entropy or apply for a role we are placing on behalf of a client, we will collect and use your Personal Data to assess your application, verify the information you have provided, communicate with you about the opportunity and, where you accept an offer, onboard you. Specifically:

- we may share your CV and assessment outputs with the relevant client where you have consented to such sharing;
- we may conduct reference checks, qualification verification and, where relevant and lawful, background checks;
- we will retain unsuccessful application data for 24 months from last contact unless you instruct us otherwise, in case future suitable roles arise; you may opt out at any time; and
- where the role requires processing of Sensitive Personal Data (e.g., medicals), we will seek your explicit Consent and apply heightened safeguards.

13. CCTV and Office Visitors

Our office may use CCTV for security, safety and crime-prevention purposes. Notices are displayed at points of entry. Recordings are retained for 30 to 90 days unless required for investigation or legal proceedings. Access to recordings is restricted to authorised personnel.

14. Third-Party Links

Our website may contain links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy practices. We encourage you to read the privacy policy of every website you visit.

15. Children

Our services are not directed at, and we do not knowingly collect Personal Data from, persons under the age of 18. If we become aware that we have collected Personal Data from a minor without verifiable parental or guardian Consent, we will delete it without undue delay unless retention is required by law.

16. Personal Data Breach

If we become aware of a Personal Data Breach that is likely to result in a real risk of harm to you, we will notify the ODPC without undue delay and, in any event, within 72 hours, and we will notify you without undue delay where the breach is likely to result in a high risk to your rights and freedoms, in line with Sections 43 of the Data Protection Act.

17. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. The latest version, together with its effective date, is available on our website. Where changes are material, we will take additional steps to bring them to your attention. Your continued use of our website or services following the effective date of an updated Policy indicates your acceptance of the changes.

18. Contact and Complaints

For any question about this Privacy Policy or to exercise your rights, please contact us at info@entropy.ke. You also have the right at any time to lodge a complaint with the Office of the Data Protection Commissioner.

Approval

This Policy has been reviewed and approved by the Board of Directors of Entropy Africa Industries Ltd as a binding policy of the Company. It is effective from the date stated below and remains in force until superseded by a subsequent Board-approved version.



George Jilani
Chairman, Board of Directors Entropy Africa Industries Ltd
Effective Date: 1 January 2026