Ejoobi — Privacy Policy

How we protect your personal information across the Ejoobi ecosystem

Version: 3.0
Effective date: 8 May 2026
Last reviewed: 8 May 2026
Responsible Party / Controller: Ejoobi (Pty) Ltd, Registration No. 2016/324519/07, 161 Allan Road, Glen Austin, Midrand, 1685, South Africa.
Information Officer: The Information Officer, Ejoobi (Pty) Ltd, admin@ejoobi.co.za, +27 10 285 0834.
EU/UK Representative: Where required by GDPR Article 27 or UK GDPR, our representative will be appointed and named at this address before any large-scale processing of EU/UK residents commences.
Information Regulator (SA): JD House, 27 Stiemens Street, Braamfontein, Johannesburg 2001 POPIAComplaints@inforegulator.org.za

This Privacy Policy explains, in plain language, what Personal Information we collect about you, how and why we use it, who we share it with, how long we keep it, where it is stored, and the rights you have under the laws that protect it. If anything is unclear, email admin@ejoobi.co.za and we will explain.

1. Scope of this Policy

This Policy applies to every product, application, website, mobile interface, USSD channel, WhatsApp service, application programming interface, and AI-assisted feature operated by Ejoobi (Pty) Ltd or by an affiliate, partner, or white-labelled instance under licence from Ejoobi (the “Platform Ecosystem”). The Policy also covers Ejoobi-branded services and any future Ejoobi product.

It applies whether you are a Job Seeker, a Recruiter, an Employer, a Partner, an Administrator, or simply a Visitor to one of our public pages.

It should be read together with our Terms and Conditions, our Cookie Policy, and our Acceptable Use Policy. Where we act as an Operator (POPIA) or Processor (GDPR) for a Recruiter, Employer, or Partner, the Data Processing Agreement applies in addition.

In some circumstances Ejoobi acts as a Responsible Party/Controller in respect of Personal Information processed for the operation, security and administration of the Platform Ecosystem. In other circumstances, Ejoobi acts as an Operator/Processor on behalf of Recruiters, Employers or Partners who determine the purposes and means of processing. The role applicable to a particular processing activity will be communicated where required by law.

2. Laws that govern our processing

Our default benchmark is the Protection of Personal Information Act 4 of 2013 ("POPIA"). Where any of the following also apply to a particular processing activity, we comply with them as well:

- the EU General Data Protection Regulation 2016/679 ("GDPR") where we offer Services to data subjects in the European Economic Area or monitor their behaviour there;
- the United Kingdom GDPR and the UK Data Protection Act 2018, on the same basis;
- the Electronic Communications and Transactions Act 25 of 2002 ("ECTA");
- the Consumer Protection Act 68 of 2008 ("CPA");
- the Cybercrimes Act 19 of 2020;
- the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("RICA");
- the Financial Intelligence Centre Act 38 of 2001 ("FICA"), where we conduct customer due-diligence on Recruiters and Employers; and
- any other law of South Africa or, where applicable, of the data subject's home jurisdiction.

Where this Policy uses POPIA terminology (Responsible Party, Operator, Personal Information), the GDPR equivalents (Controller, Processor, personal data) apply for users to whom GDPR applies.

3. Key definitions

- **Personal Information / personal data** — information about an identifiable, living natural person and (under POPIA) identifiable existing juristic persons; includes name, contact details, identity number, employment history, CV content, photographs, location data, online identifiers, device data, and inferred data.
- **Special Personal Information / special category data** — information about a person's health, biometrics, religion, race, political views, trade-union membership, sex life or sexual orientation, and (under POPIA s.26) criminal behaviour.
- **Processing** — any operation we perform on Personal Information, including collection, storage, viewing, organisation, transmission, disclosure, anonymisation, and deletion.
- **Responsible Party / Controller** — the party that decides why and how Personal Information is processed. Ejoobi is the Responsible Party for the data we collect on the Platform Ecosystem in our own right.
- **Operator / Processor** — a third party that processes Personal Information on behalf of, and on the documented instructions of, a Responsible Party.

4. What we collect, why we collect it, and our lawful basis

We only collect Personal Information that is adequate, relevant and not excessive for the purpose for which it is processed. We collect it directly from you, from sources you have made public (for example, professional networking profiles you have linked to your account), and from accredited

verification partners (for due-diligence on Recruiters and pre-employment checks consented to by Job Seekers).

Where Personal Information is collected directly from you, Ejoobi will provide the information required by section 18 of POPIA, including the purpose of collection, whether the supply of information is voluntary or mandatory, the consequences of failing to provide the information, any planned cross-border transfers, and the categories of third parties with whom the information may be shared. This Privacy Policy forms part of that notification.

4.1 Job Seekers

Category	Examples	Purpose	Lawful basis (POPIA s.11 / GDPR Art. 6)
Identification	Full name, ID number or passport number, date of birth	Identity verification, fraud prevention, statutory compliance	Performance of contract; legal obligation
Contact	Cell number, email, residential address	Account communication, recruiter messaging, multi-channel CV sharing	Performance of contract; consent for marketing channels
Profile and CV	Employment history, qualifications, skills, languages, photograph (optional), portfolio links	Matching to vacancies, display to authorised Recruiters and Employers	Performance of contract; consent
Location	Province / city; precise GPS only with your permission	Showing relevant nearby vacancies	Consent
Device and usage	IP address, browser, operating system, pages viewed, session logs	Security, debugging, Service improvement, fraud detection	Legitimate interest
Inferred / AI-generated	Skills tags inferred from your CV, role-fit scores	AI-assisted matching (see clause 8)	Legitimate interest, with right to object and human review
Special Personal Information — criminal record	Declared criminal history, output of a background check	Only when you apply for a role that lawfully requires it and you have given explicit consent	Explicit consent (POPIA s.27 / GDPR Art. 9(2)(a))
Special Personal Information — health	Disability status, occupational-health declarations (only where required by the role)	Reasonable accommodation, statutory reporting	Explicit consent or substantial public interest

4.2 Recruiters and Employers

Category	Examples	Purpose	Lawful basis
Company details	Registered name, registration number, VAT number, registered address, tax-clearance status, BBBEE certificate, CIPC documents	Identity verification, due diligence (FICA where applicable)	Contract; legal obligation
Representative details	Name, title, business email, business phone of the company representative and Authorised Users	Account administration and authentication	Contract
Billing	Last-4 digits of payment card, bank reference (full card data is held by our payment-gateway provider; we do not see it)	Processing licence Fees and optional services	Contract
Usage	Login events, search queries, messaging activity, vacancy posts, audit logs	Security, billing, audit, fraud prevention	Contract; legitimate interest

4.3 Visitors

If you only browse our public pages without logging in, we collect device and usage data through cookies (see Cookie Policy) and our hosting and analytics providers. We do not link this to your identity unless you create an account.

4.4 Personal Information from third parties

We may receive Personal Information about you from: (a) accredited KYC and verification providers we engage to perform due diligence on Recruiters and Employers; (b) background-check providers, where you have given specific consent; (c) Recruiters and Employers, when they invite you to join the Platform Ecosystem under their account; (d) public sources you have linked to your profile; and (e) law-enforcement or regulatory bodies where required by law.

5. Special Personal Information — criminal record and health

We treat data about a person's criminal record and health as Special Personal Information and apply stricter safeguards. We collect or verify it only where:

- you have given specific, informed, written or click-wrap explicit consent for a particular purpose, recruiter, or employer; or

- you have applied for a role for which a check is required by law (for example, FAIS-regulated roles or roles involving children under the Children's Act 38 of 2005) or by the prospective employer.

Background-check output is generated only when an accredited verification partner runs the check. It is shared only with the requesting Recruiter or Employer. It is never visible to other Recruiters as a default profile field. You may withdraw consent at any time, and we will delete the output within thirty (30) calendar days, except where retention is required by law, regulatory obligations, litigation holds, contractual requirements, or legitimate recruitment record-keeping purposes.

6. Children

The Platform Ecosystem is intended for, and marketed to, persons aged 18 and above only. We do not knowingly collect Personal Information from anyone under 18. If we discover that we have inadvertently collected information from a person under 18, we will delete it without undue delay. If you are a parent or legal guardian and believe we have collected information about your child, contact admin@ejoobi.co.za and we will act promptly.

Where we become aware that Personal Information of a child has been submitted by a parent, guardian, employer or educational institution for lawful recruitment, internship or bursary programme, we will process such information only where permitted by applicable law and with necessary authorisations

7. Cookies, pixels, and similar technologies

We use first-party and third-party cookies and similar technologies to keep you logged in, remember preferences, measure how the Services are used, detect fraud, and (where you consent) measure marketing performance. The first time you visit, you will see a cookie banner that lets you accept, reject, or configure non-essential cookies. Full details, including the categories of cookies and how to opt out, are set out in our separate Cookie Policy.

8. AI-assisted features and automated decisions

Some Services use machine-learning and large-language-model technology to suggest matches, summarise CVs, draft messages, screen applications against criteria you have published, and detect fraud. AI Features are decision-support tools, not decision-makers.

Where an AI Feature produces a decision that has a legal effect on you or similarly significantly affects you (for example, exclusion from a shortlist, account suspension, or denial of a benefit), you have the right under POPIA section 71 and GDPR Article 22 to (a) be informed, (b) obtain meaningful information about the logic involved, (c) have the decision reviewed by a human, and

(d) contest the decision. Email admin@ejoobi.co.za with the subject line “Automated decision review” to exercise this right.

We do not use Job Seeker Personal Information, the contents of confidential Recruiter searches, or proprietary Recruiter Content to train general-purpose foundation models, and we contractually prohibit our AI processors from doing so. We may use de-identified, aggregated data to improve the matching algorithms, fraud detection, and Service performance.

9. Who we share Personal Information with

We do not sell or rent your Personal Information. We share it only with the following categories of third parties, under written contracts that impose POPIA-level (and where applicable, GDPR-level) safeguards:

9.1 Recruiters and Employers

Profile and CV data of Job Seekers is made available to Recruiters and Employers that have completed our due-diligence process and that have a bona fide vacancy. Application history, messages, and any documents you choose to attach are shared with the specific recipient you apply to.

9.2 Verification, KYC, and background-check providers

Accredited partners that verify Recruiter and Employer registration, tax compliance, and (with explicit consent) Job Seeker pre-employment checks.

9.3 Multi-cloud infrastructure providers

Hosting, storage, content-delivery, encryption-key-management, and security-monitoring providers that operate the technical infrastructure of the Platform Ecosystem. We follow a multi-cloud strategy with primary infrastructure in South Africa and a hot standby in another approved region for resilience and disaster recovery; see clause 11 for cross-border safeguards.

9.4 Communications providers

Email-delivery, SMS-gateway, and WhatsApp Business API providers that carry our notifications, one-time passwords, and CV-sharing messages.

Where notifications are delivered through third-party messaging platforms, such providers may process metadata necessary to route and deliver communications in accordance with their own privacy notices.

9.5 Payment providers

PCI-DSS compliant payment-gateway providers that process Recruiter and Employer subscription Fees and optional service charges. We do not store full card numbers.

9.6 Analytics, attribution, and advertising

Privacy-aware analytics providers (for example, Google Analytics 4 with IP anonymisation), product-analytics providers, and — only where you have consented — advertising-attribution partners. Categories and opt-out instructions are in our Cookie Policy.

9.7 AI services and model providers

Reputable AI infrastructure providers that host the matching, summarisation, and fraud-detection models we use. Such providers are contractually prohibited from using Ejoobi data to train their general-purpose models, are required to delete inputs and outputs within a defined retention window, and are bound by confidentiality and security obligations.

9.8 Professional advisers

Our attorneys, auditors, insurers, and accountants, under duties of confidentiality.

9.9 Law enforcement and regulators

Where we are legally obliged to disclose, where it is necessary to protect a person's life, rights, or safety, or where a court order requires it. We will, where lawful, give you prior notice of any such disclosure.

9.10 Corporate transactions

In the event of a sale, merger, restructuring, or acquisition of all or substantially all of our assets, we may transfer Personal Information to the buyer or successor under the same protections that apply under this Policy. We will notify affected users.

On request, we will provide you with the current list of our processors and sub-processors.

10. International transfers and multi-cloud hosting

We follow a multi-cloud strategy. Job Seeker Personal Information is stored primarily on infrastructure located in the Republic of South Africa. We maintain encrypted backup copies and a hot disaster-recovery standby with another reputable cloud provider, which may be located in the European Economic Area, the United Kingdom, or another jurisdiction recognised by the Information Regulator as offering adequate protection.

Where Personal Information is transferred outside South Africa, we rely on one or more of the lawful grounds in POPIA section 72:

- the recipient is subject to a law, binding corporate rules, or binding agreement that provides a level of protection substantially similar to POPIA;
- you have consented to the transfer (typically for AI-assisted features that route data to a non-SA region for processing, where you have been clearly informed in advance);
- the transfer is necessary for the performance of a contract with you or in your interest;
- the transfer is for the benefit of the data subject and consent is impracticable to obtain.

Where GDPR applies, we use European Commission Standard Contractual Clauses (Module 1, 2, or 3 as appropriate), supplemented by transfer-impact assessments and additional technical measures (encryption in transit and at rest, key management under our control, pseudonymisation where feasible). You may request a copy of the safeguards by emailing admin@ejoobi.co.za.

11. How long we keep your Personal Information

We keep Personal Information only for as long as we need it for the purposes described in this Policy, industry best practices or for as long as we are required to keep it by law. The default schedule is:

Data set	Retention period
Active Job Seeker account	Duration of the account plus 12 months after last login
Inactive Job Seeker account	12 months of inactivity, then anonymised and retained for statistics only
CV files and attachments	Same as account retention; deleted on request within 30 days
Criminal-record / pre-employment background-check output	12 months from the date of check, unless you request earlier deletion or the law requires longer
Recruiter / Employer account and due-diligence file	Duration of subscription plus 5 years (FICA, tax, audit)
Financial and tax records	5 years (Tax Administration Act 28 of 2011)
Authentication logs and security event logs	12 months
Marketing preferences	Until you opt out or delete your account
Communications you send to support	24 months from resolution
AI-Feature inputs and outputs (logs)	30 days, unless retained as part of a fraud or abuse investigation

When a retention period ends, we delete the data or anonymise it so it can no longer be linked to you. Encrypted backups are rotated out within three (3) months of deletion.

12. How we keep your Personal Information secure

We use appropriate technical and organisational measures, including:

- encryption in transit using TLS 1.2 or higher, and encryption at rest for databases and backups;
- role-based access controls on a need-to-know basis, with periodic access reviews;
- multi-factor authentication for administrative access;

- centralised security logging, intrusion-detection, and anomaly-detection;
- network segmentation between production, staging, and development environments;
- secrets management for API keys and credentials;
- regular vulnerability scanning and periodic third-party penetration testing;
- vendor risk-management for cloud and AI processors, including SOC 2, ISO 27001, or equivalent assurance where reasonably available;
- a documented incident-response plan, security-awareness training for staff, and confidentiality undertakings from all employees and contractors.

No system is 100 percent secure. We do not promise that the Services are immune to every conceivable attack.

13. Security compromises (data breaches)

If we have reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person, we will notify the Information Regulator and the affected data subjects as soon as reasonably possible after we have determined the scope of the compromise and taken appropriate steps to restore the integrity of the Platform Ecosystem, as required by POPIA section 22.

Where GDPR applies, we will notify the lead supervisory authority within 72 hours of awareness, where feasible, and the affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

Our notice will include, to the extent known: the nature of the compromise, the categories and approximate volume of data affected, the likely consequences, the measures we have taken or propose to take, and the steps you can take to protect yourself. Recruiters, Employers, and Partners must notify Ejoobi within 48 hours of becoming aware of any compromise involving data they have extracted from the Platform Ecosystem (see the Data Processing Agreement).

14. Your rights

You have the following rights in respect of your Personal Information. You can exercise any of them, free of charge, by emailing admin@ejoobi.co.za with the subject line “POPIA Request” (for South African data subjects) or “GDPR Request” (for EU/UK data subjects). We will respond within a reasonable time, and in any event within 30 days, unless an extension is permitted by law.

1. Right of access — you can ask whether we hold Personal Information about you and obtain a copy.
2. Right to correction — you can ask us to correct inaccurate or out-of-date information.
3. Right to deletion / erasure — you can ask us to delete information where we no longer have a lawful basis to keep it; we will tell you if a legal obligation requires us to retain it.

4. Right to object — you can object to processing based on legitimate interest, and you can object to direct marketing at any time.
5. Right to restrict processing — you can ask us to limit how we use your data while a dispute or accuracy concern is resolved.
6. Right to withdraw consent — where we rely on consent, you can withdraw it at any time without affecting the lawfulness of earlier processing.
7. Right to data portability — you can ask for a structured, commonly used, machine-readable copy of the Personal Information you have provided to us.
8. Right to refuse automated decision-making — see clause 8.
9. Right to lodge a complaint — you can complain to the Information Regulator (South Africa), to your competent EU/UK supervisory authority, or to any other authority that has jurisdiction.

We will ask for proof of identity before acting on a request. We may refuse requests that are manifestly unfounded, excessive, or that the law prevents us from fulfilling, and we will explain why if we do.

15. Marketing communications

We will only send you marketing communications where the law allows it. For Job Seekers and other natural-person users we rely on your opt-in consent under section 69 of POPIA and section 45 of ECTA, and — where GDPR applies — your consent under Article 6(1)(a). For existing Recruiter and Employer customers we may rely on the soft opt-in for similar products. Every marketing message contains an unsubscribe link, and you can opt out at any time from your account settings.

16. Accuracy of information

We take reasonable steps to ensure that Personal Information remains accurate, complete, not misleading and updated where necessary. You agree to keep the information on your profile accurate and up to date. If we find information that is verifiably false, we may suspend or remove the account concerned. We do not require you to indemnify us for honest mistakes.

17. Third-party websites and services

The Services may link to third-party sites or integrate with third-party platforms. We are not responsible for their privacy practices. We recommend you read their policies before sharing Personal Information with them.

18. Changes to this Policy

We review this Policy at least once a year and whenever there is a material change to how we process Personal Information. If we make a material change, we will tell you by email and by an in-product notice at least fourteen (14) days before the change takes effect. Continued use of the Services after the change means you accept the updated Policy.

19. Contact and complaints

Issue	Contact
General privacy questions	admin@ejoobi.co.za
Data-subject rights requests (SA)	admin@ejoobi.co.za with subject line “POPIA Request”
Data-subject rights requests (EU/UK)	admin@ejoobi.co.za with subject line “GDPR Request”
Security concerns or suspected breach	admin@ejoobi.co.za with subject line “Security”
Information Regulator (South Africa)	POPIAComplaints@inforegulator.org.za
EU lead supervisory authority	We will notify users of our lead supervisory authority once an EU representative is appointed

This Policy is drafted to comply with POPIA, ECTA, the CPA, the Cybercrimes Act, and — where applicable — the GDPR and UK GDPR. It does not replace legal advice. By using the Services you confirm that you have read and understood this Policy.