



POPIA Compliance Statement

Version 1.0.0 · Last updated 2026-04-16 · liivra.com/legal/popia-statement

This POPIA Compliance Statement is issued by Liivra (Pty) Ltd ("**Liivra**") in terms of section 18 of the Protection of Personal Information Act 4 of 2013 ("**POPIA**"). It should be read together with our full Privacy Policy (/legal/privacy_policy), which provides additional detail on how we handle your personal information.

1. Responsible Party

| Detail | Information | |---|---| | **Company name** | Liivra (Pty) Ltd | | **Registration number** | 2022/736452/07 | | **Registered address** | 20 Mirage Drive, Helderkruijn, Gauteng, South Africa 1724 | | **Website** | liivra.com (<https://liivra.com>) | | **General enquiries** | support@liivra.com |

2. Information Officer

| Detail | Information | |---|---| | **Name** | Therry Martins | | **Email** | privacy@liivra.com | | **Phone** | +27 78 716 0366 | | **Postal address** | 20 Mirage Drive, Helderkruijn, Gauteng, South Africa 1724 |

Deputy Information Officer

| Detail | Information | |---|---| | **Name** | To be appointed | | **Email** | privacy@liivra.com |

The Information Officer is registered with the Information Regulator as required by POPIA s55.

3. Purpose of Processing

Liivra processes personal information for the following specific purposes:

- Account management** — Creating and maintaining your user account, authenticating your identity, and managing your profile settings and preferences.
- Property matching** — Connecting Tenants and Buyers with suitable properties based on their stated preferences, location, and budget criteria.
- AI-powered recommendations** — Using machine-learning algorithms to analyse search behaviour and preferences to surface relevant property listings. See Section 10 for details on automated decision-making.
- AI-powered valuations** — Generating estimated property market values using machine-learning models trained on publicly available transaction data, municipal records, and listing attributes.
- Escrow management** — Operating the Liivra Pay trust account service, including receiving, holding, and disbursing funds in accordance with agreed transaction conditions.
-

Identity verification (KYC) — Verifying the identity of Users through our partner, Smile Identity, to comply with the Financial Intelligence Centre Act 38 of 2001 ("**FIC Act**") and to prevent fraud.

7. **Communication** — Sending transactional notifications (application status updates, payment confirmations, tour reminders, chat messages), service announcements, and responding to support enquiries.
 8. **Analytics and service improvement** — Understanding how Users interact with the Platform to improve features, fix bugs, optimise performance, and develop new services.
 9. **Fraud prevention** — Detecting and preventing fraudulent listings, fake accounts, payment fraud, and other abusive behaviour.
 10. **Legal compliance** — Meeting our obligations under POPIA, the FIC Act, the Tax Administration Act 28 of 2011, the Companies Act 71 of 2008, and other applicable South African legislation.
 11. **Marketing** — With your prior opt-in consent, sending promotional communications about new features, relevant listings, and platform updates. You may withdraw consent at any time.
 12. **Dispute resolution** — Investigating and resolving complaints, disputes between Users, and Liivra Pay transaction issues.
-

4. Categories of Data Subjects

We process personal information of the following categories of data subjects:

| Category | Description | |---|---| | **Tenants** | Individuals searching for rental property | | **Buyers** | Individuals or entities searching for property to purchase | | **Landlords** | Property owners or their authorised representatives listing property for rent | | **Sellers** | Property owners or their authorised representatives listing property for sale | | **Agents** | Estate agents registered with the EAAB who use the Platform to manage listings and client relationships | | **3D / Virtual Tour Creators** | Service providers who capture 360-degree tours and 3D dollhouse models of properties | | **Website visitors** | Individuals who visit liivra.com without creating an account | | **Job applicants** | Individuals who apply for employment at Liivra |

5. Categories of Personal Information

| Category | Examples | Applicable data subjects | |---|---|---| | **Identity information** | Full name, date of birth, gender, SA ID number or passport number | All registered Users | | **Contact information** | Email address, phone number, physical address | All registered Users | | **Financial information** | Bank account details, transaction records, payment history, Liivra Pay balances | Users who transact through the Platform | | **Biometric information** | Selfie photographs for liveness detection, facial geometry data (processed by Smile Identity, not stored by Liivra) | Users who undergo KYC verification | | **Location information** | GPS coordinates (with permission), IP-derived approximate location | All Users | | **Behavioural information** | Search queries, listings viewed, listings saved, filters applied, time on page, feature interactions | All Users | | **Device information** | Device model, operating system, app version, browser type, unique device identifiers, push notification tokens | All Users | | **Content** | Listing descriptions, photographs, virtual tour media, chat messages, application documents | Landlords, Sellers, Agents, Tenants, Buyers | | **Professional information** | EAAB registration number, Fidelity Fund Certificate details, agency name | Agents |

6. Recipients of Personal Information

We share personal information with the following categories of recipients. All third-party recipients are bound by data processing agreements requiring them to protect your information:

6.1 Service providers

| Recipient | Purpose | Country | |---|---|---| | **Supabase** (database) | Hosting account data, listings, applications, transactions | Cloud (configurable region) | | **Firestore / Google Cloud** | Authentication, push notifications, media storage, analytics, crash reporting | United States | | **Paystack** | Card and mobile payment processing | South Africa / Nigeria | | **Ozow** | EFT payment processing | South Africa | | **Stitch Pay** | Account-to-account payment processing | South Africa | | **NOWPayments** | Cryptocurrency payment processing | EU | | **Smile Identity** | Identity verification and liveness detection | Nigeria / Cloud | | **PostHog** | Product analytics | United States / EU | | **Sentry** | Error and crash monitoring | United States | | **Resend** | Transactional email delivery | United States | | **Microsoft Clarity** | Session recording and heatmaps (web) | United States | | **Replicate** | AI photo enhancement (object removal, virtual staging, sky replace) — only when you opt in to a paid polish on a Listing photo | United States |

6.2 Other Users

Landlords, Sellers, and Agents see your name and contact details when you enquire about a Listing or submit an application. Tenants and Buyers see Listing content and Agent contact details.

6.3 Regulatory and legal

We may disclose personal information to the South African Revenue Service, the Financial Intelligence Centre, the Information Regulator, law enforcement, or courts where required by law or legal process.

7. Cross-Border Transfers

Some of our service providers process personal information outside South Africa (see table in Section 6.1). In accordance with POPIA s72, we ensure that cross-border transfers are subject to:

- Adequate data protection laws in the receiving country; or
- Binding agreements (data processing agreements with standard contractual clauses) that provide a level of protection substantially similar to POPIA; or
- Your explicit consent, where applicable.

We conduct transfer impact assessments for new service providers and review existing arrangements annually.

8. Security Measures

Liivra implements the following technical and organisational measures to protect personal information, as required by POPIA s19:

Technical measures

- **Encryption in transit:** All data transmitted between User devices and our servers is encrypted using TLS 1.2 or higher.
- **Encryption at rest:** Databases, file storage, and backups are encrypted using AES-256 or equivalent industry-standard encryption.
- **Access controls:** Role-based access control (RBAC) with the principle of least privilege. Multi-factor authentication required for all internal systems.
- **Network security:** Firewalls, intrusion detection, and DDoS mitigation.

- **Secure development:** Code reviews, dependency scanning, and security testing in our development pipeline.

Organisational measures

- **Data protection training:** All employees and contractors receive POPIA awareness training upon onboarding and annually thereafter.
 - **Access logging:** All access to personal information systems is logged and auditable.
 - **Vendor management:** Third-party service providers are assessed for security practices before engagement and bound by data processing agreements.
 - **Incident response plan:** Documented procedures for detecting, containing, assessing, and reporting data breaches.
-

9. Data Breach Notification

In the event of a security breach that compromises personal information, Liivra will:

1. **Contain** the breach and commence an investigation immediately upon discovery.
 2. **Assess** the risk of harm to affected data subjects.
 3. **Notify the Information Regulator** as soon as reasonably possible, and in any event within **72 hours** of becoming aware of the breach, as required by POPIA s22.
 4. **Notify affected data subjects** as soon as reasonably possible after notifying the Information Regulator, providing:
 - A description of the breach.
 - The categories of personal information affected.
 - Measures we have taken or plan to take.
 - Recommendations for steps you can take to protect yourself.
 - Contact details for further information.
 5. **Document** the breach, including its effects and remedial measures taken, regardless of whether notification to the Information Regulator was required.
-

10. Automated Decision-Making

Liivra uses automated processing in the following areas:

10.1 AI property matching

Our matching algorithm analyses your preferences, search behaviour, and listing attributes to generate personalised property recommendations. This is automated processing that produces recommendations, but it does not make binding decisions about your access to services.

10.2 AI price estimates

Our machine-learning models generate estimated property values. These estimates are informational and do not constitute binding valuations, financial advice, or automated decisions with legal effect.

10.3 Content moderation

Automated systems screen listing content for policy violations. Flagged content is reviewed by a human moderator before any action is taken.

10.4 Fraud detection

Automated systems may flag suspicious account activity or transactions for review. Flagged accounts are reviewed by our trust and safety team before any suspension.

Your rights regarding automated decisions

In accordance with POPIA s71, you have the right to:

- **Be informed** that a decision has been made solely by automated means.
- **Request information** about the logic involved in the automated decision.
- **Request human intervention** — you may ask for a human to review any automated decision that significantly affects you.

To exercise these rights, contact privacy@liivra.com with the subject line "Automated Decision Review".

11. How to Exercise Your Rights

Under POPIA s23-25, you have the right to:

| Right | Description | How to exercise | |---|---|---| | **Access** (s23) | Request confirmation of what personal information we hold about you and obtain a copy | In-app: Profile ' Settings ' Privacy & Data ' Request Data Export. Email: privacy@liivra.com | | **Correction** (s24) | Request correction of inaccurate, incomplete, or misleading information | In-app: Profile ' Edit Profile. For other data: email privacy@liivra.com | | **Deletion** (s24) | Request deletion of personal information no longer necessary for the purpose collected | Email: privacy@liivra.com (subject to legal retention requirements) | | **Objection** (s11(3)) | Object to processing based on legitimate interest, or object to direct marketing | In-app: Profile ' Settings ' Privacy & Data ' Marketing Preferences. Email: privacy@liivra.com | | **Data portability** | Request your data in a structured, machine-readable format | Email: privacy@liivra.com | | **Restrict processing** | Request that we limit processing while a complaint is being resolved | Email: privacy@liivra.com | | **Withdraw consent** | Withdraw previously given consent at any time | In-app or email as above |

Process

1. Submit your request via the in-app privacy settings or by email to privacy@liivra.com.
2. We will verify your identity before processing your request (we may ask for proof of identity).
3. We will respond within **30 days** of receiving your verified request.
4. If we cannot fulfil your request (e.g., due to legal retention obligations), we will provide written reasons.
5. There is no fee for exercising your rights, unless a request is manifestly unfounded or excessive.

Postal requests

You may also submit requests by post to:

The Information Officer Liivra (Pty) Ltd [Registered office address — to be confirmed]

12. Complaint to the Information Regulator

If you are not satisfied with how we have handled your personal information or your data subject request, you have the right to lodge a complaint with the **Information Regulator (South Africa)**:

| Office | Details | |---|---| | **Head office** | JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001 | | **Postal** | P.O. Box 31533, Braamfontein, 2017 | | **Complaints email** | complaints.IR@justice.gov.za | | **General enquiries** | infoereg@justice.gov.za | | **Phone** | 010 023 5207 | | **Website** | <https://infoeregulator.org.za> (<https://infoeregulator.org.za>) |

13. Data Retention Summary

| Data category | Retention period | Legal basis | |---|---|---| | Account data | Life of account + 5 years after deletion | Companies Act s24 | | Financial records | 7 years from transaction date | Tax Administration Act s29 | | KYC documents | 5 years from last transaction or account closure | FIC Act s22 | | Chat messages | Life of account + 1 year | Contractual necessity | | Analytics data | Anonymised after 24 months | Legitimate interest | | Crash/error logs | 90 days | Legitimate interest | | Marketing consent records | Duration of consent + 1 year | POPIA compliance |

Full details are provided in our Privacy Policy (/legal/privacy_policy), Section 8.

14. Policy Review

This POPIA Compliance Statement is reviewed:

- **Annually**, as part of our regular compliance review cycle.
- **Upon material changes** to our data processing activities, the Platform's features, or applicable law.
- **Following a data breach**, to incorporate lessons learned and updated procedures.

Changes will be communicated via email and in-app notification. The current version is always available at liivra.com/legal/popia_statement (https://liivra.com/legal/popia_statement) and within the Liivra mobile app under Profile ' Legal ' POPIA Statement.

15. Contact

For any questions regarding this POPIA Compliance Statement or the processing of your personal information:

- **Information Officer:** privacy@liivra.com
- **General support:** support@liivra.com
- **Legal:** legal@liivra.com