Ubuntu Explorer – POPIA Compliance & Data Protection Framework

1. Purpose

This document outlines Ubuntu Explorer's approach to compliance with South Africa's **Protection of Personal Information Act (POPIA, Act 4 of 2013)**. The aim is to protect the personal data of **tourists (users)** and **SME owners (partners)** by ensuring lawful, secure, and transparent data practices.

2. Scope of Data Collected

Tourists (Users):

- Name, email, contact number (account creation).
- Location data (for recommendations & SOS feature).
- Travel preferences, in-app activity, feedback.
- Emergency contacts (optional).

Business Owners (SMEs):

- Business profile (name, address, contact).
- Financial details (for payouts/commissions).
- Analytics (traffic, customer engagement).

3. POPIA Principles in Action

- **Lawfulness & Fairness**: Data collected only for tourism services (e.g., safety, recommendations, SME visibility).
- **Purpose Limitation**: Data is not repurposed for unrelated marketing or third-party resale.
- **Minimality**: Only essential data collected; no unnecessary sensitive info.
- **Consent & Transparency**: Users must opt-in; privacy policy accessible in app + website.
- **Security Safeguards**: Encryption, access controls, and incident response protocols in place.

- **Data Subject Rights**: Tourists & SMEs can access, correct, or request deletion of their data at any time.
- **Accountability**: Ubuntu Explorer designates a **Data Protection Officer (DPO)** to oversee compliance.

4. How We Keep Data Safe

Technical Safeguards:

- **Encryption**: All personal and financial data encrypted at rest (AES-256) and in transit (TLS 1.3).
- **Anonymisation**: Location & analytics data anonymised after use to prevent tracking individuals.
- **Access Control**: Role-based access ensures only authorised staff can view sensitive data.
- **Cloud Security**: Hosted on secure cloud infrastructure (AWS/Azure) with built-in compliance tools.
- **Monitoring & Alerts**: Real-time intrusion detection and 24/7 log monitoring.

Organisational Safeguards:

- **Data Protection Officer (DPO)** appointed to enforce compliance.
- **Employee Training**: Staff undergo annual POPIA and cybersecurity training.
- **Incident Response Plan**: Any breach is logged, reported to the Information Regulator, and affected users are notified within 72 hours.
- **Third-Party Vetting**: All vendors (payment gateways, cloud providers) must meet POPIA + GDPR-level security standards.

5. Tourist Data Safety Measures

- **SOS & Location Sharing**: Stored only for the duration of the emergency. Automatically deleted after 24 hours.
- **Emergency Contacts**: Saved only with explicit consent. Not shared outside the safety function.

- **Travel Preferences**: Used solely for AI recommendations; anonymised when aggregated for analytics.
- **Gamification Data**: Progress, quiz scores, and achievements are stored under user profiles but are non-sensitive.

6. Business Owner Data Safety Measures

- **Business Profiles**: Public-facing details (address, offerings) are voluntarily submitted by SMEs.
- **Financial Data**: Bank/payment details encrypted and tokenised; Ubuntu Explorer never stores raw card data.
- **Analytics**: Visitor numbers and engagement stored in aggregate — no personal tourist data is shared directly with SMEs.
- **Access Controls**: Only the SME owner has dashboard access; Ubuntu Explorer staff can only view anonymised statistics.

7. Data Retention Policy

- **Tourist Data**: Retained for the active period of account + 2 years for legal/tax purposes. Can be deleted upon request.
- **Business Data**: Retained for duration of SME partnership. Deleted within 6 months of account termination.
- **Backups**: Encrypted backups stored for disaster recovery, rotated every 30 days.

8. Cross-Border Processing

- If data is stored outside South Africa (e.g., in cloud servers), Ubuntu Explorer ensures compliance with **Section 72 of POPIA**, requiring “substantially similar protection” as in South Africa.
- Cloud providers must be POPIA/GDPR compliant.

9. User Rights Under POPIA

Tourists & SME owners may:

1. Request access to their personal data.
2. Request correction of inaccurate data.
3. Withdraw consent at any time.
4. Request deletion (“right to be forgotten”).
5. Lodge a complaint with the Information Regulator.

10. Governance & Accountability

- **Data Protection Officer (DPO)**: Oversees compliance, audits, and incident response.
- **Annual POPIA Audit**: Conducted to test safeguards and update policies.
- **Policy Review**: Updated annually or when laws change.