baobab – Data Processing & Retention Policy

Effective Date: October 24, 2025
Entity: Virtual Operative Services OÜ
Registered Office: Tallinn, Estonia
Operating Jurisdiction: Republic of South Africa
Compliance: POPIA (South Africa), GDPR (EU), Electronic Communications and Transactions Act (ECTA)

1. Purpose

The purpose of this policy is to:

1. Establish how **Virtual Operative Services OÜ** processes, stores, and protects user data collected through baobab.
2. Define retention periods for all types of user and system data.
3. Ensure compliance with **POPIA**, **GDPR**, and other applicable data protection laws.
4. Minimize risk of unauthorized access, loss, or misuse of data.

2. Scope

This policy applies to:

- All personal data and user-generated content within baobab (posts, comments, conflict reports).
- Technical metadata, device information, and usage data.
- Payment and subscription data.
- Administrative and moderation logs.
- All employees, contractors, and third-party service providers with access to baobab data.

3. Data Collection

Data types collected and processed include:

1. **Personal identifiers:** Name, email, phone number, account ID.
2. **Authentication data:** Password hashes, tokens, verification documents (ID or passport, if required).
3. **Content data:** Posts, comments, media uploads, location-tagged reports.
4. **Technical data:** Device ID, OS version, IP address, browser type, crash logs.
5. **Payment data:** Subscription plan, payment processor confirmations, billing metadata.

4. Data Processing Purposes

Data is processed for:

- **Service delivery:** Account authentication, content display, tiered access.
- **Security and moderation:** Detecting abuse, fraud, or illegal content.
- **Research and analytics:** Aggregated usage patterns for app improvements.
- **Legal compliance:** Responding to lawful requests from authorities, regulatory obligations.
- **User support:** Responding to inquiries, troubleshooting, and account management.

5. Data Storage

5.1 All data is stored on **Google Firebase (EU servers)**, ensuring GDPR-level security standards.

5.2 **Encryption:**

- Data at rest: AES-256 encryption.

- Data in transit: TLS 1.2+ encryption.
- Payment information: Tokenized and never stored in plaintext on baobab servers.

5.3 **Access controls:**

- Role-based access (limited by function).
- Two-factor authentication for administrative accounts.
- Audit logging of all data access and modifications.

6. Data Retention Periods

Data Type	Retention Period	Notes
Account info (name, email, phone)	Active + 12 months after deletion	Allows recovery, compliance, and audit
User-generated content	Active + 12 months anonymized after deletion	Retains historical reports for civic data purposes
Payment data	5 years	Required by financial compliance laws
Technical logs and crash reports	2 years	For security, diagnostics, and performance improvements
Moderation logs	3 years	Legal evidence and policy compliance

6.1 After the retention period, data is securely deleted or anonymized irreversibly.

6.2 Backup copies are retained for disaster recovery only, encrypted, and automatically purged after 30 days.

7. Data Access and Control

7.1 Only authorized personnel with a legitimate operational need may access personal data.

7.2 Access to user-generated content is restricted to:

- Moderation team (for review, flagging, and compliance).
- Analytics team (for aggregated, anonymized reporting).

7.3 Users can manage, download, or request deletion of their data via the in-app settings or by contacting **privacy@virtualopservices.com**.

8. Data Deletion and Anonymization

8.1 **Account deletion:** When a user deletes their account:

- Personal identifiers are removed within 24 hours.
- User-generated content is anonymized for research or reporting purposes.

8.2 **Anonymization process:**

- Names, emails, phone numbers, and exact locations are removed.
- Content is retained for trend analysis without identifying users.

8.3 **Emergency deletion:**

- In cases of legal order or breach, affected data can be deleted immediately from active and backup storage.

9. Data Sharing

9.1 Data is shared only with:

- Service providers (Firebase, Google, Apple, Stripe) under binding confidentiality and security agreements.
- Moderation and research partners using anonymized data.
- Law enforcement or government authorities when legally mandated.

9.2 No user data is sold, traded, or shared for marketing purposes outside of baobab's operational scope.

10. Cross-Border Data Transfers

10.1 Personal data may be transferred from South Africa to **EU-based Firebase servers**.

10.2 Transfers comply with GDPR Chapter V and POPIA Section 72:

- Standard Contractual Clauses (SCC) in place with EU service providers.
- Appropriate technical and organizational measures ensure equivalent protection.

11. Data Breach Management

11.1 Any suspected or confirmed data breach triggers:

- Immediate containment and assessment.
- Notification to affected users within 72 hours (if personal data at risk).
- Reporting to South African authorities (Information Regulator) and, where relevant, EU authorities.
- Remedial actions to prevent recurrence.

12. Security Measures

- Role-based access control and two-factor authentication.
- AES-256 encryption at rest, TLS encryption in transit.
- Regular internal and third-party security audits.
- Periodic key rotation and access log reviews.

- Strict access controls for third-party service providers.

13. User Responsibilities

Users must:

- Keep login credentials confidential.
- Report suspected security breaches or unauthorized access.
- Avoid sharing personal information of other users without consent.

Failure to comply may result in suspension or termination of access.

14. Policy Review and Updates

This policy is reviewed annually or whenever:

- Legal or regulatory requirements change.
- Operational procedures or technology are updated.
- Significant new data processing activities are introduced.

Updated versions are posted in-app and on the baobab website with the new **Effective Date**.

15. Contact for Data Matters

For inquiries, complaints, or exercising your rights under POPIA/GDPR:

Data Protection Officer
Virtual Operative Services OÜ
Email: privacy@virtualopservices.com
Registered Office: Tallinn, Estonia
Operating Address: Cape Town, South Africa