CORPORATE POLICY

Data Protection and Confidentiality Policy

POLICY NUMBER	OPES-POL-12
VERSION	IFC
POLICY OWNER	Managing Director (as data controller)
APPROVED BY	Board of Directors, 6 March 2025
EFFECTIVE DATE	6 March 2024
NEXT REVIEW	12 months after approval
APPLIES TO	All OPES personnel and anyone processing information on OPES's behalf

1. Purpose

Clients trust OPES with commercially sensitive information, and individuals trust us with their personal data. This policy sets out how OPES protects both.

2. Legal framework

- Ghana: Data Protection Act, 2012 (Act 843). OPES will register with the Data Protection Commission as required.
- Norway and the EU: the General Data Protection Regulation (GDPR), as incorporated into Norwegian law, for personal data processed by OPES's Norwegian presence or relating to individuals in the EEA

3. Data protection principles

OPES processes personal data in line with these principles:

1. **Lawful, fair and transparent:** we have a lawful basis and tell people how their data is used
2. **Purpose limitation:** we use data only for the purposes for which it was collected
3. **Data minimisation:** we collect only what we need
4. **Accuracy:** we keep data accurate and up to date
5. **Storage limitation:** we keep data no longer than necessary
6. **Security:** we protect data against unauthorised access, loss or damage
7. **Accountability:** we can demonstrate compliance

4. Rights of individuals

Individuals may request access to, correction of, or deletion of their personal data, and may object to certain processing. Requests should be sent to operations@opesafrica.com and will be answered within the time required by law.

5. Confidential business information

- Client information is used only for the engagement it was provided for, and is shared only with those who need it
- Confidentiality agreements are signed before receiving sensitive client information, and their terms are followed
- Information barriers are applied where required by the Conflicts of Interest Policy (OPES-POL-03)
- Confidentiality obligations continue after personnel leave OPES

6. Information security

OPES applies controls in line with ISO/IEC 27001 good practice, including:

- Multi-factor authentication on email and cloud systems
- Encrypted devices and secure, company-managed storage; no client data on personal accounts
- Access granted on a need-to-know basis and removed promptly when roles change
- Regular backups and software updates
- Annual awareness training on phishing and data handling

7. Third-party processors and transfers

Service providers that process personal data for OPES must sign a data processing agreement. Personal data is transferred outside Ghana or the EEA only where the law permits and appropriate safeguards are in place.

8. Data breaches

Any actual or suspected data breach must be reported to the Managing Director immediately. OPES will assess the breach, contain it and notify the regulator, affected individuals and clients where required. Under the GDPR, notifiable breaches must be reported to the supervisory authority within 72 hours.

9. Retention

Records are kept in line with OPES's retention schedule. Financial and compliance records are kept for at least seven years, and other personal data is deleted when no longer needed.

10. Breaches and review

Breach of this policy may lead to disciplinary action. The policy is reviewed every 12 months.