

Protection of Personal Information (POPI) Policy

1. Purpose

The purpose of this policy is to ensure that COG Resourcing processes personal information responsibly, in compliance with the Protection of Personal Information principles, to protect the privacy rights of individuals and maintain data security.

2. Scope

This policy applies to all employees, contractors, and third parties who collect, store, process, or handle personal information on behalf of **COG Resourcing**, including data relating to:

- Employees
- Clients and customers
- Suppliers and vendors
- Partners and beneficiaries

3. Definition of Personal Information

Personal information means any information relating to an identifiable, living individual, including but not limited to:

- Name, ID number, passport number
- Contact details (phone, email, address)
- Employment and financial records
- Health or biometric data
- Any other data that can identify an individual directly or indirectly

4. Data Processing Principles

COG Resourcing commits to processing personal information:

- Lawfully, fairly, and transparently
- Only for specified, explicit, and legitimate purposes
- Minimally, collecting only what is necessary
- Accurately and kept up to date
- Securely, protected against unauthorized access, loss, or damage
- Retained only for as long as necessary and then securely destroyed or anonymized

5. Consent and Rights of Data Subjects

- Personal information will not be collected or processed without the data subject's explicit consent unless otherwise legally permitted.
- Data subjects have the right to:
 - Access their personal information
 - Request correction or deletion of inaccurate data
 - Withdraw consent where applicable
 - Lodge complaints about data handling

6. Security Measures

To protect personal data, the company will implement:

- Physical, electronic, and organizational safeguards (e.g., access controls, encryption)
- Regular staff training on data protection and privacy
- Secure storage and transmission methods

7. Third-Party Data Sharing

- Personal information will only be shared with third parties who comply with data protection standards and for legitimate business purposes.

- Data sharing agreements or contracts will be established to ensure third-party compliance.

8. Data Breach Management

- Any suspected or actual breach of personal data must be reported immediately to the **Data Protection Officer (DPO)** or designated person.
- The company will investigate, mitigate, and notify affected individuals or authorities as required by law.

9. Employee Responsibilities

- All employees must understand and comply with this policy.
- Unauthorized disclosure or misuse of personal information may lead to disciplinary action, including termination.

10. Policy Review

This policy will be reviewed at least annually or in response to changes in data protection laws or organizational requirements.