POPIA POLICY

Company Name: Tradecloud (Pty)Ltd
Version: 1.0
Effective Date: 01/10/2025
Approved By: COO
Next Review Date: 01/10/2026

---

1. Purpose

The purpose of this policy is to ensure that Tradecloud (Pty)Ltd complies with the requirements of the **Protection of Personal Information Act (POPIA)** and processes personal information lawfully, fairly, and transparently.

This policy outlines how personal information is collected, stored, used, protected, and disposed of within the organization in relation to its **import, export, Software and technology services**.

---

2. Scope

This policy applies to:

- All employees, contractors, consultants, and third-party partners.
- All processing activities involving personal information of customers, employees, suppliers, and third parties.
- All business units including software systems, online platforms, import/export management systems, and customer relationship tools.

---

3. Legislative Framework

This policy is based on:

- **Protection of Personal Information Act, 2013 (Act No. 4 of 2013)**
- **ISO/IEC 27001:2022** (Information Security Management Systems)
- **Electronic Communications and Transactions Act (ECTA)**
- **Promotion of Access to Information Act (PAIA)**

---

4. Definitions

Term	Definition
Personal Information	Any information relating to an identifiable natural or juristic person, including names, contact details, ID numbers, location data, online identifiers, etc.

Term	Definition
Processing	Any operation concerning personal information, including collection, storage, modification, retrieval, use, and destruction.
Information Officer	The person responsible for ensuring compliance with POPIA within the organization.
Data Subject	The person to whom personal information relates.
Operator	A third party who processes personal information on behalf of the company.

---

5. POPIA Principles and Commitments

Tradecloud (Pty)Ltd adheres to the eight principles of lawful processing:

1. **Accountability:** The company ensures compliance with POPIA in all operations.
2. **Processing Limitation:** Personal information is collected only for legitimate business purposes.
3. **Purpose Specification:** Information is processed only for specific, lawful, and explicitly defined purposes.
4. **Further Processing Limitation:** Information will not be processed in a manner incompatible with the purpose for which it was collected.
5. **Information Quality:** The company ensures that personal data is accurate, complete, and up to date.
6. **Openness:** Data subjects are informed of the collection and purpose of their data.
7. **Security Safeguards:** Appropriate technical and organizational measures protect personal data against unauthorized access, alteration, loss, or destruction.
8. **Data Subject Participation:** Individuals have the right to access and correct their personal information.

---

6. Types of Personal Information Collected

Category	Examples	Purpose
Client Information	Names, contact details, company registration numbers, VAT details	For service delivery, invoicing, support, and compliance
Employee Information	ID, address, banking, medical, emergency contact	For HR, payroll, and statutory compliance
Supplier / Vendor Information	Company and contact details, bank accounts	For payment, procurement, and contract management

Category	Examples	Purpose
Online User Data	IP address, device info, login data	For system access, monitoring, and cybersecurity
Import/Export Documentation	Customs info, permits, declarations	For compliance and transaction processing

---

7. Collection and Processing of Personal Information

- Information is collected directly from data subjects or authorized representatives.
- The company will not collect information beyond what is necessary for the purpose intended.
- Data subjects will be informed of the purpose and use of their data upon collection.
- Any processing by third parties (operators) is governed by data processing agreements.

---

8. Information Security and Safeguards

To ensure confidentiality, integrity, and availability of personal data, the company applies controls aligned with **ISO 27001**:

- Access control (role-based access, strong authentication, and password management).
- Encryption of stored and transmitted data.
- Regular data backups and secure offsite storage.
- Network security monitoring and incident response procedures.
- Physical security controls (access cards, CCTV, locked storage).
- Employee awareness training on data privacy and cybersecurity.

---

9. Sharing and Disclosure of Information

Personal information will only be shared:

- When legally required or permitted.
- With third-party service providers (operators) under written data processing agreements.
- With government authorities for customs and compliance purposes.
- Across international borders only when adequate data protection measures are in place.

---

10. Retention and Disposal

- Personal information is retained only for as long as necessary to fulfil its purpose or as required by law.
- Secure disposal methods (digital wiping, shredding) are used when information is no longer required.
- Data retention schedules are maintained and reviewed annually.

---

11. Rights of Data Subjects

Data subjects have the right to:

- Request access to their personal information.
- Request correction or deletion of inaccurate data.
- Object to processing under specific circumstances.
- Lodge complaints with the Information Regulator.

Requests must be submitted in writing to the **Information Officer**.

---

12. Roles and Responsibilities

Role	Responsibility
Information Officer	Ensures overall compliance with POPIA, handles data subject requests, and reports incidents.
Deputy Information Officer(s)	Supports compliance and handles operational aspects.
Department Managers	Ensure compliance within their units.
All Employees	Protect personal data handled in the course of their duties.

---

13. Data Breach Management

In the event of a data breach:

- The incident must be reported immediately to the Information Officer.
- The Information Officer will assess and contain the breach.
- The **Information Regulator** and affected data subjects will be notified as required by POPIA.
- Root cause analysis and corrective actions will be documented.

---

14. Training and Awareness

All employees undergo periodic POPIA awareness training. Refresher sessions are conducted annually to ensure ongoing compliance and awareness of updates or regulatory changes.

---

15. Policy Review

This policy will be reviewed **annually** or upon significant change in legislation, business operations, or systems affecting personal data processing.

---

16. Approval

Information Officer: _____
Signature: _____
Date: _____