

Customer Personal Info Impact Assessment

PIIA Guide

This guide aligns with the Protection of Personal Information Act (**POPIA**), Act 4 of 2013. Section 4 (Conditions for lawful processing) and Section 19 (Security safeguards) require responsible parties to identify and manage risks to personal information.

Step 1: Identify Personal Information

Document all personal information processed. Include purpose, storage location, access control, and legal basis for processing (**POPIA Section 11**).

List all personal information you collect. Include what data, who it belongs to, why it is collected, where it is stored, and who has access.

Create a simple spreadsheet with columns:

- What data? (Name, ID number, email, banking details, employee records, etc.)
- Who is it about? (Customers, staff, suppliers)
- Why do we collect it?
- Where is it stored?
- Who has access?

Example

Data	Who	Why	Stored Where	Access
ID Number	Customers	FICA	Google Drive	Admin only
Payroll info	Employees	Salary processing	Payroll system	HR

👉 If you don't know where it lives, that's your first vulnerability.

Step 2: Map Data Flows

Identify how data is collected, transferred, stored, and shared. Assess cross-border transfers (**POPIA Section 72**).

Document how data is collected, where it moves, who it is shared with, and whether it leaves the country.

Ask:

- How is it collected? (Website form, email, WhatsApp, paper form?)
- Where does it go next?
- Is it shared with anyone? (Accountant, IT provider, CRM system?)
- Is it transferred outside South Africa?

Example of a simple data flow diagram:

Customer → Website Form → Email → CRM → Accountant

👉 Anywhere data moves = potential risk.

Step 3: Identify Risks

Evaluate risks including unauthorised access, weak passwords, phishing, improper retention, and third-party processor risks (**POPIA Section 21**).

Ask what could go wrong. Consider hacking, accidental disclosure by you or your suppliers, weak passwords, lack of encryption, and excessive retention.

For each type of data, ask:

- Could this be hacked?
- Could staff accidentally email it to the wrong person?
- Is it stored unencrypted?
- Is it backed up?
- Is it kept longer than necessary?

Common small business risks:

- Shared passwords
- No 2FA
- Staff using personal Gmail
- Customer info in WhatsApp chats
- Open Google Drive folders
- Old employee records never deleted

Step 4: Rate the Risks

Use a traffic light system to prioritise mitigation actions.

- Low – Minor impact
- Medium – Some harm possible
- High – Serious financial or reputational damage

Example:

Risk	Impact	Rating
Shared admin password	High	●
Paper forms in locked cabinet	Low	●
No laptop encryption	High	●

👉 Focus first on ● items.

Step 5: Implement Safeguards & Action Plan

Apply appropriate technical and organisational measures (**POPIA Section 19**). Assign responsibility and deadlines.

For every ● and ● risk, assign:

- *What must be done?*
- *Who is responsible?*
- *Deadline?*

Example:

Risk	Action	Owner	Deadline
Shared password	Implement password manager + 2FA	IT	30 days
Old staff records	Implement 3-year retention policy	HR	14 days

Review Frequency

1. Annually at minimum.
2. When introducing new technology or vendors.
3. After any security incident (Section 22 breach notification).
4. When business processes change.

Keep It Simple – 1 Folder

Maintain:

- PIIA register (spreadsheet)
- Risk register
- Action plan
- Last review date

If the regulator ever asks, you can show:

“We identified risks, assessed impact, and took corrective action.”

👉 That demonstrates reasonable level of accountability under POPIA.