POPI Compliance Checklist

Eight compliance gaps we see most often in South African SME infrastructure — and what to fix first.

---

01 **Information officer not registered**

Every organisation processing personal information must register an information officer with the Information Regulator. Most SMEs either skip this entirely or haven't formally registered, which is a compliance gap on its own regardless of anything else below.

02 **No data processing record**

You need a written record of what personal information you hold, where it's stored, why you collect it, and who has access. Without this, you can't answer a subject access request or a Regulator enquiry with any confidence.

03 **No retention policy**

Personal information kept indefinitely, past the point it's actually needed, is itself a POPI violation — not just a housekeeping issue. A defined retention and deletion schedule needs to exist and actually be followed.

04 **Third-party processor agreements missing**

Any vendor that touches your customers' or staff's personal information on your behalf — payroll providers, marketing tools, hosting companies — needs a signed operator agreement in place, not just a verbal understanding.

05 **No breach response plan**

POPI requires notifying the Regulator and affected data subjects when a breach occurs. If there's no defined process for identifying, containing, and reporting a breach, that notification won't happen on time when it matters.

06 **Weak access controls**

Shared logins and flat access — where anyone in the business can see any customer's information — make it impossible to demonstrate the 'reasonable technical and organisational measures' POPI requires.

07 Unencrypted backups or email archives

Personal information sitting in an unencrypted backup or an old email archive is still personal information under POPI. It needs the same protection as your production systems, not an exemption because it's 'just a backup'.

08 No consent trail

Where you rely on consent to process personal information — marketing lists are the common case — you need to be able to show when and how that consent was given. Without a trail, you can't prove it was ever obtained.

Not sure which of these apply to you?

Rev2IT reviews infrastructure for South African SMEs against POPI, PCI-DSS and GDPR, backed by a 99.5% uptime SLA. Book a free infrastructure review at rev2it.com, or get in touch directly at enquiries@rev2it.co.za.