

POPIA Quick Checklist for Small Businesses

Free from Kontrak. General guidance only — not legal advice.

Before you collect any personal information

- ☐ [] Appoint and register an Information Officer with the Information Regulator.
- ☐ [] List what personal information you collect (names, emails, ID numbers, photos, IP addresses).
- ☐ [] Write down why you need each item — collect only what you need.

On your website

- ☐ [] Publish a privacy policy naming your Information Officer and contact details.
- ☐ [] Add an unticked opt-in box for marketing emails (POPIA section 69).
- ☐ [] Show a cookie notice if you use analytics or advertising pixels.
- ☐ [] Use HTTPS on every page with a form.

In your client contracts

- ☐ [] Include a POPIA clause explaining how client data is used and protected.
- ☐ [] Get written consent before using client photos in your portfolio or ads.
- ☐ [] State how long you keep files and how clients can ask for deletion.

Day to day

- ☐ [] Store client files on password-protected, backed-up systems.
- ☐ [] Use a written agreement with anyone who processes data for you (assistants, editors, VAs).
- ☐ [] Have a plan to notify clients and the Regulator if data is lost or hacked.
- ☐ [] Delete personal information you no longer need.