Organizations have until July 1, 2021, to fully comply with the Protection of Personal Information Act, 2013 (POPIA). POPIA compliance is a lengthy project, so your organization should begin as soon as possible.

The checklist on the following pages will help your organization kickstart its POPIA compliance journey.
Information audit

Conduct an information audit to determine:
- What categories of personal information your organization processes
- Why it is processed (what's the purpose?)
- Where and how you store the personal information
- Who you share personal information with

Organizational impact assessment

Conduct an organizational impact assessment to identify:
- How POPIA impacts your organization
- Adequate measures needed to comply with POPIA’s eight conditions for lawful processing of personal information
- Any glaring compliance gaps

Consult with your legal and IT experts to determine the best approach to resolving these issues.

Legal ground for processing

Processing personal information is unlawful under POPIA unless you can justify it according to one of the listed grounds in Section 11(1) of POPIA.

Appoint an information officer

Your organization must appoint an information officer and register this officer with the Information Regulator. Your information officer should be an expert on data protection who can monitor POPIA compliance, assess data protection risks, and cooperate with the Information Regulator.

Provide notice

Per section 18 of POPIA, responsible parties must inform data subjects that their personal information is being collected, the reason for the collection, how the information will be processed, and with whom it will be shared, amongst other things. This information should generally be provided to data subjects at the time you collect their personal information.
Contracts with service providers

Any service providers processing personal information on your behalf ("operators") must comply with POPIA. Your contracts with such service providers must include sufficient data protection guarantees and appropriate security measures. Your organization can be held liable for your service providers' non-compliance with POPIA.

Data subject rights requests

Data subjects have various privacy rights under POPIA. Your organization must have a process to address requests from data subjects to exercise these rights.

Security measures

Your organization must implement appropriate technical and organizational measures to protect personal information against loss, damage, and unauthorized access and destruction.

Personal information breaches

If the security of the personal information you are entrusted with is compromised, your organization must notify the Information Regulator of the compromise as soon as reasonably possible following the incident's discovery. Your organization should have a procedure for detecting, responding to, and investigating these security compromises.

Awareness and training

Training should be provided to all employees to ensure that they understand your organization's POPIA obligations. Employees or departments that process personal information on a day-to-day basis should receive further intensive training.

Retention and deletion

Your organization should have a set process to deal with the deletion or destruction of personal information at the end of its life cycle, in compliance with Section 14 of POPIA.
Direct marketing
Your organization is prohibited from processing personal information of a data subject for unsolicited direct marketing by means of electronic communication unless the data subject has given their consent to the processing or if the data subject is a customer of your organization. Your organization’s mailing lists must also contain an easily identifiable “opt-out” or “unsubscribe” link so that data subjects can withdraw their consent to receiving emails and other marketing materials at any time.

PAIA manual
If your organization is required to have a Promotion of Access to Information Act of 2000 (PAIA) manual under Section 51 of PAIA, your organization must provide information on the records held and the process to be followed to request access to such records.

Transborder information flows
Your organization will only be allowed to send personal information outside of South Africa under strict conditions in accordance with Chapter 9 of POPIA.

Personal information impact assessment
Although not mandated by POPIA, we recommend that your organization conduct a personal information impact assessment to identify, analyze, and minimize risks to personal information when you undertake specific projects.

DISCLAIMER
The information contained in this checklist does not include an exhaustive list of all POPIA compliance requirements and does not constitute legal advice. Accordingly, any organization using this checklist may not rely on it as such. Like most privacy laws, POPIA is complex and open to interpretation. It is strongly recommended that organizations seek professional legal advice on how to comply with POPIA.
ABOUT VERASAFE

VeraSafe offers a complete solution to help your organization comply with POPIA. Our specialist privacy professionals and IT security experts are uniquely placed to provide a holistic approach to compliance.

Visit our POPIA Compliance page for more information about VeraSafe's POPIA Compliance Program.

U.S. based callers: 1-888-376-1079
Callers from outside U.S.: +1-617-398-7067
www.verasafe.com