

February 22, 2021

Understanding the impact of POPI Act Compliance on your business



Personal information has become one of the most powerful commodities in the modern world. In this new age of data privacy and processing information, every time you process personal information you will be subject to either local or foreign data privacy and protection laws (such as POPI or GDPR).

All businesses in South Africa need to be fully compliant with the Protection of Personal Information Act (POPI Act) by 1 July 2021 as the Information Regulator will start enforcing compliance one year after the commencement of the POPI Act in July 2020.

We understand that becoming POPI compliant can be a time-consuming process and some businesses may find it challenging as they don't know where to start with the process.

To assist with some direction, we have identified the top **10 indicators to evaluate your POPI compliance**:

1. Have you been subject to an independent POPI audit?

Identifying all the risks relating to organisational and technical aspects. This should include identifying all the role players, types of information, information life cycle, etc.

2. Have you identified the type of information?

Is the information securely processed, stored and shared according to the POPI-compliance requirement?

- o Do you process personal information relating to children?
- o Do you process special personal information?
- o Are you an Operator, *Responsible Party*, or both?

3. Have you identified the purpose of processing information?

This includes identifying what industry and business activities you are involved in. Who are your consumers and which additional regulations do you need to comply with?

- o *Certain industries have additional requirements, for example the medical industry.*
- o Do you sell goods or deliver a service?
- o Who are your customers, and do they need to be *GDPR compliant*?

4. Have you appointed an Information Officer?

The Information Officer has certain responsibilities in the organisation to ensure that-

- o a compliance framework is developed, implemented, monitored and maintained.
- o a POPI audit is conducted so that adequate measures and standards are applied.
- o internal measures are developed, with a system to process requests or access information.

5. Awareness and training

The Information Officer must ensure that internal (staff and management) awareness seminars are conducted.

6. Data loss, data breach procedures, incident response policies

- o Identify threats and data flow throughout the network and systems.
- o Detect unauthorised access to, loss of and misleading information.
- o Make sure that all role players are notified and informed of procedures.

7. Policies/Agreements

- o Do you transfer legal responsibility to IT service providers for when a data breach occurs?
- o Develop and implement procedures and policies for all employees and customers/suppliers?

8. Consent

Data should only be processed for the purpose for which it was acquired and for the period required. This data must be deleted once it has served its purpose. *The data subject should always sign a consent form.* This includes employees, clients, third parties, suppliers, etc. The data subject may withdraw consent at any time, in which case all information should be deleted.

9. Cross-border/third-party access

There are restrictions for cross-border data transfer when sending data out of South Africa. These restrictions are dependent on the laws of the country to which the data is being transferred.

10. PAIA Manual

- o Does your organisation need a Promotion of Access to Information Act (PAIA) manual?
- o Ensure that your PAIA manual includes the necessary information and is submitted to the Human Rights Commission annually.

POPI Act non-compliance

Businesses that do not comply with the Act will be paying fines of up to R10 million and can be blacklisted. Their officials could even face imprisonment for periods ranging from 12 months to 10 years. The Information Regulator will also stop your organisation from processing information to ensure that you are unable to do business.

SERR Synergy assist businesses in ensuring that personal information processing is according to legislation, while simultaneously serving the needs your business may have with such data.

We provide a full range of Information Compliance service offerings, be it compiling Data and Information Protection Reports, drafting of required Data Privacy policies, updating your agreements to handle data considerations, advising on internal data handling requirements or understanding what exact data privacy role you fulfil.

Reputational damage for noncompliance is a material risk which may lead to directors being declared unfit to be a director in terms of the *Companies Act*.

Be prepared for this new age of data privacy and protection, feel free to *contact us* for more information.

About the Author: Retha van Zyl completed her B.Com Hons (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 and currently holds the title 'Information Compliance Advisor'. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA Manuals to the Human Rights Commission. She also compiles the Data and Information Protection Report to identify risks associated with information security and drafts Information Security policies for procedural compliance in each department within an organisation.

©SERR Synergy, www.serr.co.za