ACTUARIAL SOCIETY OF SOUTH AFRICA

POPIA CHECKLIST

WHAT IS THE PURPOSE OF POPIA?

The purpose of the act is to provide individuals and companies in South Africa with more control and visibility of how their personal data is handled by organisations that have access to it.

From July 1st 21 organisations that have access to personal data are accountable for how they process that personal data. They must:

- only process it only for the purpose specified;
- only for as long as is needed;
- only process personal information in a way that tries to ensure that that personal data is accurate, in a way that it transparent (as demonstrated in a privacy policy, for example);
- use appropriate technical and organisational measures to protect the personal data they have
- allow the data subject to know what information an organisation has about them; and
- allow for requests by the data subject to delete that information.

TERMS USED IN POPIA

"data subject"- the person (natural or juristic) whose personal data is being processed

"operator" the organisation processing the personal information on behalf of the responsible party

"personal information" any information that can identity a data subject

"responsible party" the organisation that decides and controls the manner in which the personal data is processed

Here is a simple checklist of key actions a company should consider under POPIA.

1. APPOINT AN INFORMATION OFFICER RESPONSIBLE FOR POPIA COMPLIANCE:

Organisations must appoint an Information Officer (who must be registered with the Regulator) who is responsible for compliance with **POPIA**. The Information Officer will deal with any privacy requests made to the organisation and cooperate with the Information Regulator on investigations and compliance.

2. IDENTIFY THE LAWFUL BASIS FOR PROCESSING THE PERSONAL DATA

Organisations must process personal information only if they have a lawful basis for doing so. The most common basis for processing is contractual: i.e., you cannot fulfil your contract with a person unless you process certain personal data. For marketing, some organisations can rely on the legitimate interests basis.

3. HAVE A PRIVACY POLICY IN PLACE

A privacy policy lets website users and/or clients let them how you protect their data.

4. NOTIFY SECURITY COMPROMISES AS SOON AS REASONABLY POSSIBLE:

POPIA requires organisations to notify security compromises to the Regulator and impacted data subjects if there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorised person. Such notification must be made as soon as reasonably possible after the discovery of the compromise.

5. HAVE A WRITTEN CONTRACT WITH ANY DATA OPERATOR

POPIA requires organisations to have a written contract with the operator/data processor to ensure that the operator has security measures in place for the protection of personal information.

6. RESPOND TO DATA SUBJECTS' DATA ACCESS AND RECTIFICATION REQUESTS

Under the **POPIA**, data subjects have the right to access their data and know which third parties who have access to the information. Additionally, data subjects can request to correct or delete their information. Organisations must respond to such requests as soon as reasonably practicable.

7. ENSURE ADEQUATE LEVEL OF PROTECTION IN CASES OF CROSS BORDER DATA TRANSFERS

An organisation cannot transfer personal information to a third party in a foreign country unless one of the following conditions is fulfilled:

- There exists an adequate level of protection. In other words, recipients are subject to a law, binding corporate rules or a binding agreement providing an adequate level of protection that upholds principles similar to **POPIA**.
- The data subject has consented to transfer,
- The transfer is necessary for the performance of a contract between the data subject and the data controller,
- The transfer is necessary for the performance of a contract concluded in the interest of the data subject, or
- The transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject.

8. MAINTAIN THE DOCUMENTATION OF ALL DATA PROCESSING

POPIA requires organisations to maintain the documentation of all data processing operations under its responsibility. Such documentation helps organisations demonstrate compliance to the Regulator.

Please note that this guide is intended as general guidance on new legislation and is not a replacement for tailored legal advice specific to your organisation's needs.