EVERSHEDS SUTHERLAND

8 steps to POPIA compliance!

How to make sure your business is POPIA compliant

POPIA requires organisations to adopt a new approach to privacy, and the use and protection of personal information, and to integrate the principles of data protection into their business processes.

1 Develop Project Team

- assign responsibility for driving POPIA compliance within your organisation and develop a strong POPIA compliance team
- determine whether the POPIA compliance strategy will be led at group level or within individual operating companies
- secure board approval for the resources necessary to deliver your POPIA compliance project
- ensure board and management buy-in and support for the POPIA compliance project

2 Data Mapping

- understand and map your personal information processing activities
- create clear documentary records of the processing activities under your responsibility
- update your implementation plan, having verified it against your data mapping findings

3 Gap Analysis

- analyse all policies, procedures and data processing activities against the requirements of POPIA
- consider your organisation's appetite for risk on data protection compliance matters
- produce a report to the highest level of management which identifies compliance gaps and recommends options for remedial action (including details of the anticipated resources required, timescales for completion and priority levels)
- prioritise areas of most risk when implementing solutions

4 Information Officer

- appoint the information officer and, if required, deputy information officers for the organisation
- register the information officer with the information regulator (when this functionality on the information regulator's website goes live)

5 Third Party Engagement

- audit your suppliers, subcontractors, and vendors, and renegotiate their contracts to ensure that all POPIA prescribed operator terms are suitably covered
- ensure that all new suppliers are appointed on POPIA compliant contracts
- establish a supplier due diligence policy, and prepare appropriate checklists and paperwork to document the results of due diligence
- consider the impact of POPIA exposure on other provisions of your contracts (e.g. liability)

6 Updating Policies and Privacy Documentation

- update existing policies and create new policies to address compliance gaps identified during gap analysis
- prepare processing notices, consent wording, record retention policies, subject access request policy, data protection policies etc

7 Implementing Procedures

- introduce and embed privacy by design templates and data protection impact assessments (DPIAs)
- update procedures for dealing with data subject rights (e.g. subject access requests, data portability requests, rectification requests, and objections)
- update security breach procedures
- conduct mock security breach reporting scenarios

8 Training

- train decision-makers and project team members prior to commencing POPIA project
- ensure that all personnel are suitably trained in their responsibilities and the requirements of POPIA and compliance therewith

Enforcement:

Although all organisations should ensure compliance with POPIA as everyone has the right to privacy, it is also important to note that failure to comply with POPIA could result in fines of up to **R10 million,** jail time and adverse reputational and financial consequences.

For more information, contact:

Grant Williams
Partner

grantwilliams
@eversheds-sutherland.com

Kelly Hutchesson
Senior Associate

kellyhutchesson
@eversheds-sutherland.com

Key concepts

Need-to-know elements of POPIA

Scope

POPIA applies to the processing of personal information of both natural and juristic persons, whether by automated or non-automated means, in South Africa. There are certain exclusions, including where:

- the processing is by non-automated means (i.e. on paper) and it does not form part of a filing system
- the process is purely for household or personal activity
- the personal information has been anonymised

It is important to note that GDPR only applies to the processing of personal information of natural persons, whereas POPIA applies to the processing of both natural and juristic persons (e.g. companies and trusts), but extends to the processing of the personal data of EU citizens outside of the EU.

Accountability: A responsible party is responsible for, and must to able to demonstrate, compliance with the principles relating to the processing of personal information

Consent: Consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to them. Implied consent and pre-ticked boxes will no longer be valid

Data minimisation: Personal information that a party processes must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed

Mandate required for operators: Responsible parties must have a written contract in place with operators, governing matters including data security, international data transfers, appointment of sub-processors, and security breach notification. If there is a security breach at the operator, the responsible party may receive a fine if there is no contract in place.
This is different to the position under the GDPR, where operators (processors) have direct statutory obligations when processing on behalf of the responsible parties (controllers)

International transfers: If data is transferred outside of South Africa, additional steps need to be taken by responsible parties to ensure that the recipient is subject to a law, binding corporate rules, or binding agreement, that provides adequate protection for the data.

Data subject rights

Subject access requests: Data subjects have the right to request a broad scope of information, including details of:

- the safeguards that the data responsible party has in place for international data transfer
- the period for which the responsible party envisages retaining their personal information

In most cases, the information requested by a data subject must be provided without undue delay, and in any event within 'a resonable time' of receipt of the request. Confirming whether or not the responsible party holds personal information about a data subject must be given free of charge, but an organisation may charge a 'prescribed fee' to provide a description of the personal information being processed. The information regulator has not prescribed any fees to date.

Erasure: Personal information must be erased without undue delay, where:

- processing the data is no longer necessary
- consent is withdrawn and there is no other legal reason for processing
- the individual objects and there is no overriding legal reason to continue processing
- data is unlawfully processed
- erasure is required for compliance with another law

Direct marketing: A data subject has the right not to have their personal information used for purposes of direct marketing.

Profiling and automated decisions: Data subjects have the right not to be subject to a decision evaluating personal aspects relating to them which is based solely on automated processing, and which produces legal or other significant effects concerning them (e.g. online credit applications or e-recruiting practices)

Rectification: Individuals have the right to require a responsible party to rectify inaccurate personal data concerning him or her without undue delay

Restriction of processing: Individuals have the right to restrict processing where:

- the accuracy of the personal information is contested by the data subject (where the restriction will apply during the period enabling the responsible party to verify the accuracy of the personal information)
- the processing is unlawful and, the data subject requests the restriction of the use of their personal information instead of erasure
- the responsible party no longer needs the personal information for the purposes of the processing, but they are required by the data subject in connection with any legal claims
- the data subject has objected to processing pursuant to the right to object (in which case the restriction will apply for the period necessary to determine whether the legitimate grounds of the responsible party override those of the data subject)

Right to object: Individuals have a right to object, on grounds relating to their particular situation, at any time, to processing of personal information which is based on performance of a public law duty or legitimate interest grounds, *if they can show legitimate grounds for their objection*

Procedural requirements

Privacy by design: A responsible party must, at the time that the means of processing is determined and at the time of processing itself, implement appropriate technical and organisational measures which are designed to:

- implement data protection principles (e.g. data minimisation)
- integrate necessary safeguards to meet the requirements of POPIA and protect the rights of data subjects

Appointing a processor: Organisations must only use operators that provide sufficient guarantees that the processing will meet the requirements of POPIA and all processing by operators must be governed by a contract or other binding legal act which contains obligations on the operator to safeguard the data. Additionally, an operator cannot engage another operator (e.g. a sub-processor) without prior specific or general written authorisation of the responsible party and, the operator must flow down the same provisions as it has in place with the responsible party

Security breach reporting: Organisations must provide notice of a security breach, in the case of responsible parties to the regulator and affected data subjects, as soon as reasonably possible after detection

Data Protection Impact Assessments: Data protection impact assessments must be conducted where a type of processing (in particular using new technologies) is likely to result in a high risk to the rights and freedoms of the data subject

eversheds-sutherland.co.za

DTUK000565_05/21