Information Officers Association

Helping you understand

POPIA

appointing an information officer

Your guide to the Protection of Personal Information Act

www.informationofficers.co.za

Contents

The importance of protecting personal information

The Protection of Personal Information Act No 4 of 2013, (POPIA) commenced on 1 July 2020. All public and private bodies, with few specific exceptions, are required to comply with the POPIA requirements. Personal information is any information that relates to a living, identifiable natural person or an existing juristic person (e.g. a company). In order to process such information, one must comply with the information processing conditions contained in POPIA and enable data subjects to exercise the related rights.

Selecting an information officer

POPIA compliance requires responsible parties to register their information officers with the Information Regulator. When selecting an information officer, responsible parties must be mindful of their own lability with respect to non-compliance with the conditions for lawful processing of personal information and all the measures that give effect to such conditions.

There are numerous provisions in the Protection of Personal Information Act that require the responsible party to act in a reasonable manner. The standard to determine whether a responsible party has acted reasonably is that of objective foreseeability. In other words, would a reasonable person have foreseen the harm?

Any deviation from the standard of foreseeable harm establishes negligence, irrespective of whether the damage is due to the act of the responsible party, a staff member or a service provider. Clearly, a responsible party can be held liable even though there is no apparent fault on his or her own.

The burden of proof rests with the responsible party to demonstrate that he or she did properly and continuously assess the risk and take all the measures necessary to mitigate the risks from appointing an inexperienced information officer.

The responsible party must carefully consider the skill and experience an information officer will require to discharge his or her duties in the context of the processing operations of the organisation for which the responsible party is accountable. Selecting the right person for appointment and registration as an information officer is crucial.

Responsible parties and information officers are designated prescribed officers under the Companies Act, 2008. Prescribed officers have the same liability as directors, and therefore are liable in accordance with the principles of the common law relating to reach of a fiduciary duty, for any loss, damages or costs sustained by the company as a consequence of any breach by the director of a duty contemplated in the Companies Act, or was calculated to defraud a creditor, employee, shareholder, or another fraudulent purpose.

Appointing an information officer who does not have the necessary experience and skill puts both the responsible party and information officer at risk. Responsible parties are expected to foresee the consequences of appointing an information officer who is not capable of “encouraging compliance, by the body, with the conditions for the lawful processing of personal information, deal with requests made to the body, and working with the Regulator in relation to investigations concerning prior authorisations”.

Where a responsible party has appointed an information officer who does not have sufficient experience and skill, the responsible party is obliged to provide the information officer with adequate resources, training, and access to external expertise that can assist him or her fulfil his or her duties. Failure to do so could be viewed by some as negligence.

Who is the information officer?

Regardless of its size or nature, POPIA requires that every organisation has a responsible party and an information officer. Even the smallest entities with just one person, are required to have a responsible party and an information officer. This will ensure data subjects of that entity can exercise their rights by holding someone accountable for non-compliance and having a point of contact and assistance, to lodge a complaint and seek compensation for non-compliance with the conditions.

Unfortunately, when the same person is both the responsible party and the information officer, there is a conflict of interest. Consequently, as soon as it is practically possible to separate these roles, the information officer role should be separated from the responsible party.

POPIA, by default, designates the head of any private body as the Information Officer. In section 1 of POPIA, it defines the “information officer” in relation to a private body as “the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act” ("PAIA"). PAIA, in turn, defines the “head”, in relation to a private body and in the case of a juristic person, to be the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or the person who is acting as such or any person duly authorised by such acting person.

A chief executive officer, or equivalent officer of a juristic person, can authorise any other person to perform the duties of an Information Officer. POPIA does not prescribe who the chief executive officer can appoint, leaving it open for the chief executive officer to designate a person internal or external to the organisation as information officer.

When deciding on whom to appoint, the chief executive officer should keep in mind both the needs of the responsible parties and other stakeholders, specifically the data subjects who might place a high value on the independence of the information officer. Should the data subject doubt the independence of the information officer, he or she is more likely to go directly to the Information Regulator for assistance, and consequently a more costly outcome could result from the instance of non-compliance.

Registering an information officer

A responsible party must designate a named information officer in order to comply with POPIA. This will enable the Regulator and data subjects to easily identify the contact person who is appointed to assist them with their requests.

A responsible party can register more than one information officer in order to comply with POPIA. This would be preferable in organisations where the nature of some processing or technology is complex and technical. It will be difficult for a responsible party to demonstrate that he or she did not act negligently by appointing an information officer who doesn't have the relevant skill and experience to:

- understand the processing of personal information
- recognise the impact on data subject rights, or
- determine the technical and organisational measures that most effectively can counter the risks to data subjects.

Often the skill and experience needed by an information officer for complex business processes will not be available in-house. In such instances responsible parties will need to engage external persons to undertake the duties of an information officer.

Accessibility of an information officer

A primary duty of the information officer is to assist data subjects make requests and seek settlement from the responsible party, for non-compliance with the conditions for the lawful processing of personal information. Consequently, information officers must be generally

available to assist data subjects. At times, particularly after a significant security breach, a large number of data subjects may submit requests for information or demand action be taken concerning the processing of their personal information. Responsible parties are required to respond to these requests within the prescribed time periods. This may be difficult where only one or two information officers have been appointed. In such instances, POPIA requires the responsible party to appoint “such number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in the Act”.

In certain instances, tens of thousands, and sometimes millions of data subjects are affected by a single interference with data subject rights. Should a large number of these data subjects request information about the interference, the responsible party may need to employ thousands of deputy information officers to assist the information officer respond to thousands or millions of data subject requests for information.

Organisations with a large number of data subjects, or a widely dispersed group of data subjects will also need to plan carefully how they will give effect to the requirement to have sufficient information officers available to be accessible, and able to assist data subjects who wish to exercise their rights.

Competence of an information officer

Information officers are expected to be knowledgeable in the requirements of:

- Protection of Personal Information Act
- Promotion of Access to information Act
- Other related South African legislation
- Business processing of personal information
- The technology stack that supports the processing of personal information
- Information governance practices
- Risks to data subjects
- Technical and organisational measures that can effectively counter these risks
- Measures that can enable data subject rights

International training programmes and certifications don’t cover these requirements.

Duties of an information officer

Regulation 4(a) requires information officers to ensure a compliance framework is developed, implemented, monitored and maintained.

Information officers should have the skills necessary to develop a compliance framework:

- Governance arrangements to oversee compliance
- Assignment of data protection roles and responsibilities
- Establishment of the legal and organisational context
- Inventory of personal information
- Documentation of processing operations
- Identification of outsourced processing
- Assessment of data minimisation
- Assessment of data protection risks
- Identification of risk treatment options.

Information officers should have the skills needed to implement a compliance framework:

- Capability to notify data subjects of the purpose for processing their personal information
- Controls for the lawful processing of personal information
- Safeguards to protect personal information
- Mechanisms that enable data subject rights
- Controls over data sharing
- Processes to handle data subject requests
- Processes to manage consent.

Information officers should have the skills needed to implement a compliance framework:

- Capability to notify data subjects of the purpose for processing their personal information
- Controls for the lawful processing of personal information
- Safeguards to protect personal information
- Mechanisms that enable data subject rights
- Controls over data sharing
- Processes to handle data subject requests
- Processes to manage consent.

Information officers should have the skills necessary to monitor a compliance framework:

- Verify that business process comply with the eight conditions
- Assess the effectiveness of information security measures
- Verify the enablement of data subject rights
- Validate operator assertions of compliance.

Information officers should have the skills necessary to maintain the compliance framework:

- Respond to incidents of non-compliance
- Detecting changes in data protection risks
- Resolve issues raised by the Regulator.

Regulation 4(b) requires information officers to ensure **personal information impact assessments**. The typical steps of a personal information impact assessment include:

- Plan the assessment
- Determine the skills needed to perform the assessment
- Define target of evaluation
- Identify stakeholders and data subjects
- Identify the relevant legal bases for processing
- Identify evaluation criteria
- Identify potential attackers.
- Evaluate the risk
- Identify and select appropriate safeguards
- Document assessment results.

Automate:

Use tools that support information officers perform their duties.

Records Management

File plan taxonomy, records register and lifecycle, multi-jurisdiction retention library, disposal workflows, litigation holds, and audit trails.

Data Breach Management

End-to-end POPIA Section 22-aligned workflow: detection, containment, risk assessment, Regulator/subject notification decisions, and documentation of remedial actions.

PAIA Annual Report

Prepare annual PAIA reporting data (financial year, request volumes and outcomes, manual publication status) and record Regulator submission references.

Personal Information Redaction

Upload documents, detect personal information (e.g. email, SA ID, phone, cards), review findings, apply redaction, and download a redacted file with audit logging.

Personal Information Discovery

Scan content, databases, filesystems, uploads, and APIs for personal information; produce risk-scored findings and discovery reports with remediation guidance.

AI Log Analyzer

Bridge to AI/runtime log analysis: sync alerts and evidence packs, and escalate high-risk events into Data Breach Management cases.

Bulk Data Subject Import & Notify

CSV import of data subjects, group assignment, contact verification, canned messages, and bulk notification (e.g. breach notices) to verified subjects only.

Learning Management (LMS)

Integrated training capability so organisations can deliver POPIA awareness and professional development courses alongside the compliance portal.

Information officer services

For more information and support, contact the Information Officers Association:

Email: info@informationofficers.co.za