



Information Officers Association

Helping you
understand

POPIA

and the
PAIA manual

Your guide to the Protection of Personal
Information Act



www.informationofficers.co.za

Contents

The importance of protecting personal information.....	1
What do these guidelines include?	2
The PAIA Manual	3
1. Contact details of the information officer	3
2. Contents of the manual as required for PAIA	4
3. Contents of the manual as required for POPIA	4
4. Availability of the PAIA Manual	6
5. Exemption	6
6. Voluntary disclosure	6
7. Method of access to a record (PAIA)	6
8. Data subject requests (POPIA)	7
9. Fees	9
Glossary and abbreviations	9

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.

POPIA compliance requires a comprehensive and ongoing focus on a broad range of operational activities that use personal information. It requires accountability and oversight (i.e. governance) of how personal information is being looked after and data subject rights are respected throughout its lifecycle.

Through the growing use of digital technologies, organisations are producing more personal information than ever before – making robust governance, safeguarding personal information, compliance with the conditions for the lawful processing of personal information and enabling data subjects to protect their personal information from processing that is not in accordance with the Act, more important than ever.

The way personal information is used and maintained is a key responsibility and is fundamental to the way responsible parties look after their staff, customers and other data subjects' rights, whether digitally or otherwise.

The Protection of Personal Information Act and its Regulations require information officers to fulfil certain responsibilities including:

- encouraging responsible parties to comply with the conditions for the lawful processing of personal information
- dealing with requests made to responsible parties from data subjects and the Regulator related to POPIA
- developing, implementing, monitoring and maintaining a compliance framework
- conducting personal information impact assessments to ensure that adequate measures and standards exist in order to comply with the conditions
- developing internal measures together with adequate systems to process requests from the Regulator, data subjects and other interested parties.

As these are legal requirements, the Information Officers Association aims to assist information officers by sharing knowledge and promoting best practices.

How these guidelines can help

The Information Officers Association has developed this best practice guideline to assist members, affiliates and other interested parties in the processing of personal information so that they can make more informed decisions and, in turn, ensure their duties are fulfilled and the rights of data subjects are respected and enabled.

This document shares current best practices relating to data protection in South Africa, as well as the most relevant current legislation, regulations and guidance available from the Information Regulator.

What do these guidelines include?

- PAIA manual.

It's recommended that you explore the information provided and review the recommended practices against your current practices.

Disclaimer: The content of this document is for guidance and illustrative purposes only. These guidelines are neither advice nor a checklist to be used prescriptively to manage data protection obligations.

The PAIA Manual

Every organisation is required to develop, monitor, maintain and make available a manual as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

The purpose of a manual is two-fold. For the Promotion of Access to Information Act (PAIA) it gives effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights; and to provide for matters connected therewith. For the Protection of Personal Information Act (POPIA), it increases transparency regarding processing operations involving personal information and may increase data subjects' trust in the processing activities and the technology used. The POPIA condition of openness requires that any information or communication relating to the processing of personal information is easily accessible and easy to understand, and that clear and plain language be used.

The specific purposes for which personal information is processed should be explicitly stated, together with details of the legal basis of doing so, and the responsible party's legitimate interest in the processing. The right to be informed, under Section 18 of POPIA, is a key part of any organisations obligations to be transparent. Section 110 requires Section 14 and 51 of PAIA to be changed to include this information in the PAIA manual. The right of access, under Section 25, adds to the transparency obligation by requiring that data subjects be given confirmation on request and access to the personal information about him, her or it that the responsible party holds. Section 14 and 51 of PAIA requires responsible parties to provide data subjects with "sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject".

1. Contact details of the information officer

The information officer (as defined for public bodies) or the head of the private body unless the responsibilities as an information officer have been delegated to another person, must make a manual available containing—

- i. postal and street address
- ii. phone and fax number
- iii. email address of the information officer (or head of the private body if none is appointed).

The purpose of these contact details is to establish the information officer (duly registered with the Regulator) as the person of contact who will deal with requests made to the body pursuant to POPIA (Section 55(b)).

2. Contents of the manual as required for PAIA

- With respect to PAIA, the responsible party must ensure that the manual contains—
- A description of the organisation's structure and functions.
- The postal and street address, phone and fax number and, if available, electronic mail address of the information officer (if a public body), the head of the body (if a private body) unless the responsibilities as an information officer have been delegated and of every deputy information officer of the body
- A description of the guide referred to in PAIA section 10, if available, and how the data subject can obtain access to it from the Information Regulator. This guide will include a description of the manner and access to records of public and private bodies. This guide will also describe the assistance available to data subjects from the information officer of a public body and all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by this Act and the Protection of Personal Information Act, 2013, including the manner of lodging an internal appeal; a complaint to the Information Regulator; and an application with a court against a decision by the information officer of a public body, a decision on internal appeal, a decision by the Information Regulator or a decision of the head of a private body.
- The latest notice regarding the categories of record of the body which are available without a person having to request access in terms of PAIA. Form E (J749) is available from the Regulator for this purpose.
- A description of the records of the body which are available in accordance with any other
- legislation. This necessitates the responsible party establishing and maintaining a register of legal obligations applicable to its processing operations (as documented under Section 17 of POPIA).
- Sufficient details to facilitate a request for access to a record of the body. Records are to be organised by category of record on each subject.
- A description of the subjects on which the body holds records.
- A description of the categories of records held on each subject. For those categories of records that are personal information, records must be retained of who are the recipients.

3. Contents of the manual as required for POPIA

Purpose of the processing.

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Steps must be taken to ensure that the data subject is aware of the purpose of the collection of the information before it is collected or as soon as reasonably practicable after it has been collected.

Data subjects must be made aware of the source, if their personal information is not collected directly from the data subject, and the name and address of the responsible party for all stages of the processing of their personal information.

Data subjects must also be made aware of:

- whether or not the supply of the information by that data subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- any particular law authorising or requiring the collection of the information;
- the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.

Using the PAIA manual for these purposes will establish a primary source for this information. This can then be supplemented with privacy notices and statements for unique instances of processing personal information.

Description of the categories of data subjects.

It would assist data subjects to better understand, and therefore reduce the number of queries and objections, if the categories of data subjects were organised by process and purpose of processing, within the functions of the organisation.

Description of categories of information, and of the information relating thereto.

It would assist data subjects to better understand, and therefore reduce the number of queries and objections, if the categories of information and the information relating thereto (data fields) were organised by process and purpose of processing, within the functions of the organisation.

Description of recipients or categories of recipients to whom the personal information may be supplied.

It would assist data subjects to better understand, and therefore reduce the number of queries and objections, if the categories of information and the information relating thereto (data fields) were organised by process and purpose of processing, within the functions of the organisation.

Planned trans-border flows of personal information.

It would assist data subjects to better understand, and therefore reduce the number of queries and objections, if the planned trans-border flows of personal information were organised by process and purpose of processing, within the functions of the organisation.

A general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

Foreseeable internal and external risks

Providing data subjects with information about the internal and external risks will assist data subjects to better understand the need for information security, and therefore reduce the number of queries and objections to the processing of their personal information.

Measures to mitigate the risks

Data subjects are entitled to receive sufficient information to allow a preliminary assessment of the suitability of the information security measures implemented by the responsible party. Insufficient information may trigger requests for more information and objections to the processing of the data subject's personal information.

Regular update of the PAIA manual

The head of a private body or information officer (in their capacity as responsible party), must on a regular basis update the manual.

4. Availability of the PAIA Manual

The manual is available—

1. on the web site of the private body;
2. at the principal place of business of the private body for public inspection during normal business hours;
3. to any person upon request and upon the payment of a reasonable amount; and
4. to the Information Regulator upon request.

5. Exemption

For security, administrative or financial reasons, the Minister may, on request or of his or her own accord, by notice in the Gazette, exempt any private body or category of private bodies from any provision of this section for such period as the Minister thinks fit.

6. Voluntary disclosure

The head of a private body (i.e. the responsible party) may, on a voluntary basis, make available in the prescribed manner a description of—

- the categories of records of the private body that are automatically available without a person having to request access in terms of this Act, including such categories available—
 - for inspection in terms of legislation other than this Act;
 - for purchase or copying from the private body; and
 - from the private body free of charge; and
- how to obtain access to such records.

The only fee payable (if any), for access to the record, is a prescribed fee for reproduction

7. Method of access to a record (PAIA)

A request for access to a record of a public or private body must be made in the prescribed form (PAIA Section 18 and 53) to the private body concerned at its address, fax number or electronic mail address.

Responsible parties must provide a secure method for returning the form, and detail the internal workflow on receipt of the form, including authorisation, change management, internal controls and audit logs.

The requester is required—

- to provide sufficient particulars to enable the head of the private body concerned to identify—
 - (i) the record or records requested; and
 - (ii) the requester.
- to identify the right the requester is seeking to exercise or protect and provide an explanation of why the requested record is required for the exercise or protection of that right.
- if, in addition to a written reply, the requester wishes to be informed of the decision on the request in any other manner, to state that manner and the necessary particulars to be so informed; and
- if the request is made on behalf of a person, to submit proof of the capacity in which the requester is making the request, to the reasonable satisfaction of the head.

Indication of the form of access required

The requester is to indicate which form of access he, she or it requires.

8. Data subject requests (POPIA)

Information and/or Access

Make the form prescribed in PAIA (Sections 18 and 53) to request confirmation or access information available to data subjects, provide a secure method for returning the form, and detail the internal workflow on receipt of the form, including any authorisation, internal controls and audit logs.

Correction

Make Form 2 - Corrections (as prescribed in the Schedule to the Regulations) available to data subjects, provide a secure method for returning the form, and detail the internal workflow on receipt of the form, including authorisation, change management, internal controls and audit logs.

Destruction

Make Form 2 – Deletions and Destructions (as prescribed in the Schedule to the Regulations) available to data subjects, provide a secure method for returning the form, and detail the internal workflow on

Objection

Make Form 1 - Objections (as prescribed in the Schedule to the Regulations) available to data subjects, provide a secure method for returning the form, and detail the internal workflow on receipt of the form, including authorisation, change management, internal controls and audit logs.

Restriction

There is no prescribed form or process in the Regulations or PAIA for the purpose of enabling data subjects to request the restriction of the processing of their personal information when the accuracy is contested (POPIA Section 14(6)(a) and (c)). Data subjects are therefore able to make this request verbally to any staff member. It is essential that the responsible party creates a form for this purpose, (instructs staff to direct data subjects to this form), and develops an internal process to handle the request.

Retain evidence

There is no prescribed form or process in the Regulations or PAIA for the purpose of enabling data subjects to request records of the processing of their personal information be retained for purposes of proof (POPIA Section 14(6)(b)). Data subjects are therefore able to make this request verbally to any staff member. It is essential that the responsible party creates a form for this purpose, (instructs staff to direct data subjects to this form), and develops an internal process to handle the request.

Assurance

There is no prescribed form or process in the Regulations or PAIA for the purpose of enable data subjects to request assurance (i.e. credible evidence) of the correction, deletion or destruction of their personal information (POPIA Section 24(2)(c)). Data subjects are therefore able to make this request verbally to any staff member. It is essential that the responsible party creates a form for this purpose, (instructs staff to direct data subjects to this form), and develops an internal process to handle the request.

Notice displayed

There is no prescribed form or process in the Regulations or PAIA for the purpose of enable data subjects, where an agreement about a correction cannot be reached, to request that information be attached in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made (POPIA Section 24(2)(d)). Data subjects are therefore able to make this request verbally to any staff member. It is essential that the responsible party creates a form for this purpose, (instructs staff to direct data subjects to this form), and develops an internal process to handle the request.

Transfer of information

There is no prescribed form or process in the Regulations or PAIA for the purpose of enabling data subjects to request the transfer of their personal information into another automated processing system (POPIA Section 14(6)(d)). Data subjects are therefore able to make this request verbally to any staff member. It is essential that the responsible party creates a form for this purpose, (instructs staff to direct data subjects to this form), and develops an internal process to handle the request.

Consent withdrawal

There is no prescribed form or process in the Regulations or PAIA for the purpose of enabling a data subject to withdraw his, her or its consent (POPIA Section 11(2)(b)). Data subjects are therefore able to make this request verbally to any staff member. It is essential that the responsible party creates a form for this purpose, (instructs staff to direct data subjects to this form), and develops an internal process to handle the request.

9. Fees

A data subject cannot be charged a fee when requesting a responsible party to confirm whether or not the responsible party holds personal information about the data subject.

If a prescribed fee is determined by the Regulator, the information officer may charge a fee upon request by any person, to provide copies of the manual.

If a prescribed fee is determined for reproduction, it will be possible for the responsible party to charge the data subject a fee for a request for the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information. Responsible parties should bear in mind that should the request for information result in an issue of non-compliance, it is likely that the data subject will request the fee back as part of the settlement.

Glossary and abbreviations

Governing body	person or group of people that governs an organisation, sets directions and holds top management to account
Interested party	person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Objective	result to be achieved
Risk	effect of uncertainty on objectives

www.info@informationofficers.co.za