Atleha-edu

Speaking life into investment decisions

www.atleha-edu.org

UNDERSTANDING POPIA
and its implications

ENSURING COMPLIANCE
as a retirement fund

KEY ROLES AND RESPONSIBILITIES
in terms of general protection principles

AN INTRODUCTION TO POPIA
FOR RETIREMENT FUNDS

VOL.10

ALSO IN THIS ISSUE: WHY IS PROTECTING PERSONAL INFORMATION IMPORTANT? | THE RISKS OF NON-COMPLIANCE
KEY TERMS AND DEFINITIONS | REGISTER FOR CPD CREDITS

This educational publication is funded by Colourfield (Colourfield is an Authorised Financial Services Provider, FSP 35113)
and the ASISA Foundation

colourfield

ASISA FOUNDATION

Atleha-edu

Speaking life into investment decisions www.atleha-edu.org

In Sesotho, when you tell someone to "Atleha" you are telling them to prosper.
Our dream for South Africans is for them to prosper through the building blocks of education and technology. By combining "Atleha", and "edu", we want to "speak life" into the dream of prosperity for the majority of South Africans.

The majority of savers in South Africa can be reached through retirement fund trustee and member education, making this the primary focus of our work at Atleha-edu. Please visit our website at www.atleha-edu.org to read our educational publications for retirement fund trustees, principal officers and MANCO members.

- Governance & Ethics For Retirement Fund Trustees
- Investment Fundamentals 1
- Investment Fundamentals 2
- Special Edition: Environmental Stewardship
- Umbrella Funds & Management Committees
- Cultural Practices
- An Introduction to Infrastructure Investments
- Retirement Funds and Risk Management
- Climate-related Financial Disclosure
- Alternative Asset Classes: Understanding Hedge Funds

Our offering:
In partnership with our implementing partners and funders, Atleha-edu is proud to offer a range of educational solutions for retirement funds and their members.

These solutions are customised and include:

- Financial Sector Code (FSC)-compliant interactive and awareness type consumer financial education programmes;
- Thought leadership webinars and events;
- Experiential workshops for deep learning experiences;
- Customised FSC-compliant consumer financial education solutions.

To learn more about our offering and to partner with us, please contact us by email info@atleha-edu.org

Our collaborators and funders in financial education and dissemination include: Alternative Prosperity Foundation, ASISA Foundation, ASISA Academy and Batseta.

alternative prosperity FOUNDATION · ASISA FOUNDATION · ASISA ACADEMY · Batseta 2021 CPD Provider

CONTENTS

04 Why is protecting personal information important?

8 Getting your POPIA strategy right

12 Demonstrating POPIA compliance and risks of non-compliance

Atleha-edu
Speaking life into investment decisions www.atleha-edu.org

Batseta 2021 CPD Provider

Please email info@atleha-edu.org or call 021 851 0091 for more information.

UNDERSTANDING POPIA AND ITS IMPLICATIONS

overview

The Protection of Personal Information Act (POPIA) establishes rights and duties that are intended to protect personal information. Its aim is to balance the legitimate needs of organisations to collect and use personal information for business and other purposes against individuals' right to privacy when it comes to their personal information. All organisations – including retirement funds and their service providers – need to be fully compliant with POPIA.

The Protection of Personal Information Act (POPIA), promulgated on 26 November 2013, promotes the right to privacy and aims to protect the personal information of consumers. POPIA has its origins within the Constitution of South Africa, given that the Bill of Rights states that "Every person has the right to privacy". Each individual's personal information forms part of this right to privacy, and POPIA is the legislation that aims to ensure that personal information is granted certain levels of protection when it comes into the hands of other private or public organisations.

Before the introduction of POPIA, individuals were susceptible to unregulated gathering, retaining, distribution and/or processing of information, as well as the unregulated use thereof. Therefore, South Africa's Parliament saw fit to introduce legislation to protect its citizens against the growing misuse of personal information.

The stated purpose of POPIA is, inter alia:

a. to promote the protection of personal information processed by public and private bodies;
b. to introduce certain conditions so as to establish minimum requirements for the processing of personal information; and
c. to regulate the flow of personal information across the borders of South Africa.

In practical terms, POPIA sets conditions for the lawful processing of personal information in order to protect the public from harm, to stop money being stolen, to stop identity theft, and generally to protect the privacy of citizens.

POPIA establishes the rights and duties that are designed to safeguard personal information. In terms of POPIA, the legitimate needs of organisations to collect and use personal information for business and other purposes are balanced against individuals' right to privacy when it comes to their personal information.

POPIA applies to a particular activity, i.e., the processing of personal data, rather than a particular person or organisation. Therefore, if you process personal data, then you must comply with POPIA. In particular, you must handle personal information in accordance with POPIA's data protection principles.

If you collect or hold information about an identifiable individual or if you use, disclose, retain or destroy that information, you are likely to be processing personal information. The scope of POPIA is very wide and it applies to almost everything you might do with an individual's personal details, including details of your employees. This means that retirement funds, as well as their service providers – such as administrators' benefit consultants – are required to fully comply with POPIA.

The enforceability of certain sections of POPIA came into effect on 1 July 2020. A grace period of 12 months from this date was given to comply with the Act. As such, all entities were expected to be fully compliant with the provisions of POPIA by 1 July 2021.

POPIA legislation

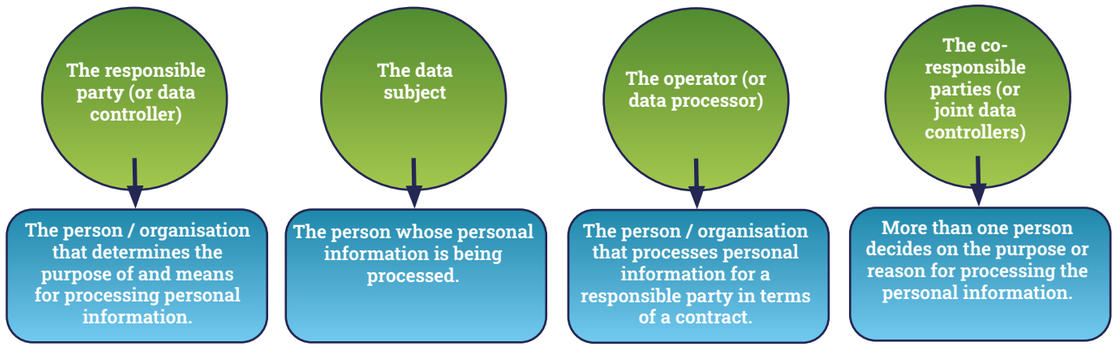
POPIA contains eight general protection principles:

1. **Accountability:** The responsible party is accountable for compliance under POPIA.
2. **Processing limitation:** The responsible party may only process personal information if, taking into account the purpose for which they are processing it, the processing is adequate, relevant and not excessive.
3. **Purpose specification:** The responsible party must collect personal information for a specific purpose, and the data subject must be aware of that purpose.
4. **Further processing limitation:** Responsible parties may only use personal information for another ("further") purpose other than the original purpose if that further purpose is compatible with the original purpose.
5. **Information quality:** The responsible party must take reasonable steps to make sure the personal information is complete, accurate, not misleading and is updated.
6. **Openness:** The responsible party must take reasonable steps to notify the data subject of certain information, such as the information being collected; the purpose for which the information is collected; whether the supply of information is voluntary or mandatory; the consequences of failure to provide information; and any particular law that applies. In the event of unauthorised accessing, processing, erasure or deletion of a data subject's personal information, the responsible party must notify the data subject, as well as the Information Regulator of this.
7. **Security safeguards:** The responsible party must have measures in place to protect the personal information collected and processed from damage, loss and unauthorised destruction, processing and access.
8. **Data subject participation:** Data subjects can ask what personal information is held about them and can ask for access and changes to their personal information.

These eight principles are explained in more depth on p.10-13.

POPIA applies to the processing of personal information, instead of a particular person or organisation. Thus, any individual or organisation processing personal information must comply with POPIA and, particularly, must handle personal information in accordance with POPIA's data protection principles.

To understand what this means, we need to understand the following POPIA-related terminology:



POPIA also includes provisions and protection around special personal information (this is personal information that is given special protection under POPIA and includes health and criminal information); children's personal information; account numbers (such as bank account numbers); personal information leaving the country; and direct marketing by means of unsolicited electronic communication.

The Information Regulator has been constituted to monitor and enforce compliance by public and private bodies with the provisions of POPIA.

POPIA therefore:

- sets out the rules and practices which must be followed when processing information about individuals and juristic persons;
- grants rights to individuals in respect of their personal information; and
- creates an independent regulator to enforce these rules, rights and practices.

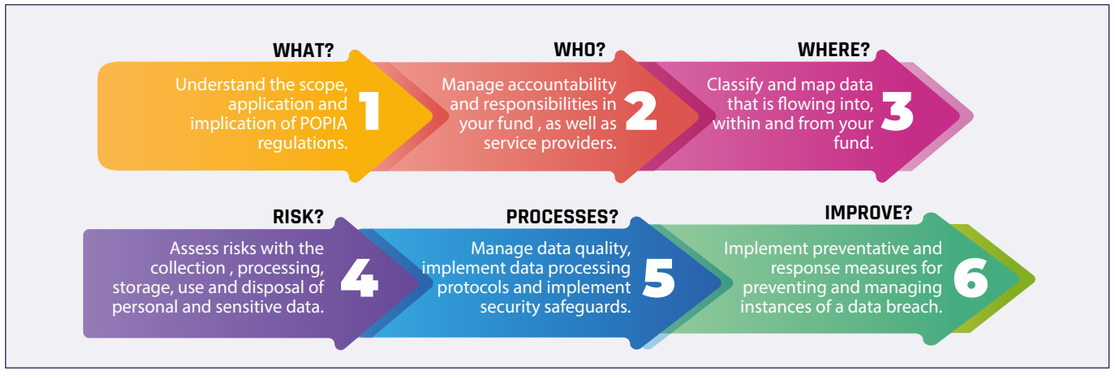
POPIA and retirement funds

Retirement funds hold and process a significant amount of personal information and related data. Such data may include employment records or financial information of fund members, members' health information and members' beneficiary details, who are sometimes minors. Funds also employ the services of third parties, such as administrators and other service providers who are responsible for processing personal information. It is the fund's responsibility to ensure that this information is protected to combat theft of member personal information, member identities, member benefits, savings or investments. It is the responsibility of the fund's board of trustees to ensure that at all times their retirement fund processes personal information lawfully, in accordance with the POPIA conditions for lawful information processing.

Matters that need to be considered by trustees when working towards POPIA compliance are:

- Written agreements and POPIA;
- Awareness and training on POPIA;
- Registering and authorising (if required) an information officer for the fund;
- Trustees' professional indemnity insurance as it relates to POPIA compliance and cyber liability insurance;
- Personal information management and security;
- Incorporation of POPIA into fund governance documents, including service provider contracts, where applicable;
- Completing a privacy impact assessment;
- Understanding and managing privacy risks related to operators.

6 key steps to POPIA compliance:



REFERENCES

- Institute of Retirement Funds Africa
- Government Gazette, POPIA, 2013
- Glacier
- Werksmans Attorneys

LEARN MORE

To learn more about this topic, please visit our website www.atleha-edu.org or contact us on 021 851 0091 to find out more about our educational workshops and events.

WHY IS PROTECTING PERSONAL INFORMATION IMPORTANT?

overview

Cybersecurity is a major issue receiving increasing attention both globally and in South Africa. One of POPIA's main aims is to protect consumers in this regard. But what exactly is cybersecurity? And how can a retirement fund and its board of trustees protect the fund and its members from cyberattacks? This article seeks to address these questions.

The advancement of technology and the internet have made goods and services increasingly more accessible. With the click of a button, people can purchase goods or pay bills from the comfort of their homes – and even on-the-go via their mobile phone. While the internet has made our lives a lot more convenient, it has also exposed society to a new type of danger: cyber threats or attacks.

Cyberattacks are usually aimed at accessing, changing or destroying sensitive information; extorting money from users; or interrupting normal business processes. Therefore, it is imperative to keep your personal information secure and, more importantly, for organisations that have your personal information on hand – such as your bank and retirement fund – to keep such personal information secure at all times. This is why legislation such as the Protection of Personal Information Act (POPIA) exists, to ensure that organisations and third parties use individuals' personal information responsibly.

In 2020 IBM, a technology company, announced in a research report that data breaches cost South African companies an average of R40.2m per breach among the organisations studied. Forty-eight percent of those incidents had malicious intent, 26% were as a result of human error and the remaining 26% were due to system errors. This study also indicated that it takes a South African organisation an average of 177 days to identify a breach and 51 days to contain that breach. By that time, considerable damage can already be wrought on the lives of many of the organisation's customers, employees and other stakeholders whose personal information the company has access to.

Big organisations are traditionally more vulnerable to cyberattacks as they are seen as larger targets for criminals, but these attacks are not exclusive to large commercial organisations. Individuals can be victims too because they often store personal information on their mobile phones and personal computers, and make use of insecure public networks. As a result of this, having a solid cybersecurity plan is essential for organisations and individuals alike. Cybersecurity is the practice of protecting systems, networks and programmes from digital attacks.

To implement a successful cybersecurity strategy, it is important to ensure that there are multiple layers of protection spread across the computers, networks or data that one intends to keep safe – the people, processes and technology in an organisation need to work together to create an effective defence from cyberattacks.

Just as the internet is vast and consists of many uses and applications, so too are the forms of cyber threats organisations need to be aware of.

"To implement a successful cybersecurity strategy, it is important to ensure that there are multiple layers of protection."

The table describes some of the more common types of cyber threats:

Malware	Malicious software variants (such as worms, viruses, Trojans and spyware) that provide unauthorised access or cause damage to a computer. These variants are often downloaded when clicking on suspicious links.
Ransomware	A type of malware that locks down files, data or systems and threatens to erase or destroy the data, as well as release sensitive information into the public domain unless a ransom is paid to the attackers.
Social engineering	A tactic used by cybercriminals to solicit sensitive information from users. It can be combined with any of the other threats listed here to make users more likely to click on links, download malware or trust malicious sources.
Phishing	A form of social engineering that tricks users into providing their own personal information. In phishing scams, emails or phone texts come from what are seemingly legitimate companies asking for sensitive information such as credit card details or login information.
Distributed denial-of-service (DDos) attacks	Trying to crash a server, website or network by overloading it with traffic, usually from multiple coordinated systems.
Man-in-the-middle attacks	An eavesdropping attack wherein a cybercriminal intercepts and relays messages between two parties in order to steal data. This is a common occurrence when users are connected to public networks.

While laws, such as POPIA, are in place to help protect individuals' personal information, there are measures that organisations – such as retirement funds and their service providers – can put in place to fend off cybercriminals. Firstly, a strong cybersecurity strategy has layers of protection to defend against cyberattacks.

The countermeasures that organisations utilise should address:

- **Critical infrastructure security** – these are practices for protecting the computer systems, networks and other systems that society relies on for national security, economic health and/or public safety.
- **Network security** – these are security measures for protecting a network from intruders. This includes both wired and wireless (Wi-Fi) connections.
- **Cloud security** – these are measures to ensure that cloud data is encrypted when it is in storage; as it travels to, from and within the cloud; and when it is being processed. This is to support customer privacy, as well as organisational requirements.
- **Information security** – these are data protection measures that secure sensitive data from unauthorised access, exposure or theft.
- **End-user education** – this involves building cybersecurity awareness across the organisation to strengthen endpoint security. Examples of this include educating employees and colleagues on the dangers of opening suspicious emails or using unknown USB devices and/or unprotected public Wi-Fi hotspots.

An additional measure to ward off cyberattacks is employing a **zero-trust security strategy**. This strategy assumes that every facet of an organisation is compromised and sets up precautions to validate every user, device and connection into the organisation for authenticity and for purpose.

Every industry has its share of cybersecurity risks – cybercriminals exploit the necessities of communication networks of almost every government and private-sector organisation. This means that the retirement industry is also susceptible to these attacks. It is therefore important for retirement funds to take these considerations into account when dealing with fund members' personal information.

A recent high-profile example of a cyberattack in South Africa, which took place in July 2021, saw Transnet "experience an act of cyberattack, security intrusion and sabotage, which resulted in the disruption of... normal processes and functions at Transnet's port facilities". Transnet declared a force majeure and was forced to manually handle container shipping processes at some of South Africa's largest ports, resulting in extensive delays due to the inefficiencies of the manual process.

REFERENCES

- **Cisco. 2021.** *What Is Cybersecurity?* [online] Available at: https://tinyurl.com/wuhw7v9h
- **iol.co.za. 2021.** *Data breach costs SA companies R40.2 million average in 2020.* [online] Available at: https://tinyurl.com/54fmn52e

LEARN MORE

To learn more about this topic, please visit our website www.atleha-edu.org or contact us on 021 851 0091 to find out more about our educational workshops and events.

Atleha-edu

Speaking life into investment decisions

www.atleha-edu.org

OVERVIEW OF PROTECTION OF PERSONAL INFORMATION ACT

ASISA FOUNDATION

colourfield

The Protection of Personal Information Act (POPIA) is South Africa's data protection law. South Africa's Protection of Personal Information Act (POPIA) has been enacted since 2013 and all "responsible parties" had until 1 July 2021 to become compliant with it. This infographic highlights some of the key elements and terms related to POPIA.

What is personal information (PI)?

- Race, gender, sex, marital status, age, religion
- Addresses, education, medical or financial history, biometric info, personal views etc.
- Trade union membership, alleged criminal behaviour, religious beliefs
- Health, sex life, political persuasion etc.

What is processing?

- Collection, usage, storage, erasure, destruction
- Alteration or distribution of information

Role players

Data Subject	Responsible Party	Operator	Regulator
Person to whom PI relates	Public/private body processing PI	Person processing PI on behalf of responsible party	Means the Information Regulator

POPIA does NOT regulate: pure household or personal activities, de-identified info, info by or on behalf of a public body, processing for journalistic purposes.

8 processing conditions

Processing of personal information is only permitted where these 8 conditions are met/ complied with.

- Accountability
- Processing limitation
- Purpose specification
- Further processing limitation
- Information quality
- Openness
- Security safeguards
- Data subject participation

Direct marketing and consent

Direct marketing	Electronic comms	Consent
Approaching a data subject in person, via mail or electronic communication to promote or offer goods and services	SMS, MMS, fax, email, voice messages, automated calling machines	Data subject must consent to direct marketing. Responsible party can only contact a data subject who has NOT previously withheld consent (opted out). Must be in a prescribed manner and form.

Regulation and compliance

Information Regulator	Monitoring and enforcing compliance	Handling of complaints	Issues codes of conduct/ guidelines
Information officer	Working with the Regulator	Dealing with POPIA requests	Developing compliance framework	Encouraging compliance

SOURCE: The Institute of Retirement Funds Africa

GETTING YOUR POPIA STRATEGY RIGHT

overview

Retirement funds are required to be POPIA compliant. This includes appointing an information officer, setting up POPIA policies and procedures and ensuring that the fund meets the eight general protection principles set out in POPIA.

The Protection of Personal Information Act (POPIA) contains eight general protection principles that responsible parties – such as retirement funds – are required to comply with each and every time they process personal information. Responsible parties must also ensure that their employees and service providers comply with these eight principles. As such, retirement fund trustees must ensure they are contracting with service providers that are POPIA compliant. In this article, the "data subject" refers to retirement fund members and the "responsible party" refers to the retirement fund.

The eight general protection principles

1 **ACCOUNTABILITY:** The responsible party is accountable for compliance under POPIA to ensure conditions for lawful processing are fully complied with.

<u>Questions to ask:</u>

- **Who will be the information officer, tasked with the responsibility of POPIA compliance within your fund?** *This individual will be held liable for non-compliance in certain situations.*
- **How will this individual ensure the fund is POPIA compliant?** *Policies and procedures must be in place.*

2 **PROCESSING LIMITATION:** The responsible party may only process personal information if, taking into account the purpose for which they are processing it, the processing is adequate, relevant and not excessive.

<u>Questions to ask:</u>

- **Was the personal information obtained directly from the data subject?** *One of the requirements of POPIA is that any personal information must be obtained directly from the data subject.*
- **Is the data subject aware that you have collected his/her information and do the necessary justifications for processing exist?** *Retirement funds don't always need to rely on consent to process personal information and may rely on other specified justifications.*
- **If the personal information has been gathered from a third party, has the data subject consented to this information being shared and used by your fund ?** *This is a requirement.*
- **Is the amount of information being processed excessive?** *Only information that is gathered for the specific purpose for which it is required may be processed.*

3 **PURPOSE SPECIFICATION:** The responsible party must collect personal information for a specific purpose, and the data subject must be aware of that purpose.

<u>Questions to ask:</u>

- **For what specific, explicit and lawful purpose is the personal information being collected?** *This purpose must be documented and adhered to.*
- **Is the data subject aware of the purpose for which the data has been collected?** *The data subject has the right to know what information you have and for what purpose it was gathered.*
- **Can you link all personal information collected to legitimate reasons for collecting?** *Personal information must only be gathered for specific, explicit and lawful purposes.*
- **For what time period may you retain specific personal information?** *Personal information may only be used for the specific purpose for which it was gathered and thereafter it must be destroyed.*
- **How will you keep track of when personal information must be destroyed?** *You will be required to account for what information you hold, for what purpose it was gathered and a date at which time that information must be destroyed.*
- **What process will be used to destroy personal information, in a manner that prevents its reconstruction, after you are no longer authorised to retain such records?** *This is an essential step in the process.*

4 **FURTHER PROCESSING LIMITATION:** Responsible parties may only use personal information for another ("further") purpose other than the original purpose if that further purpose is compatible with the original purpose.

<u>Questions to ask:</u>

- **If you intend to reuse personal information, is it in accordance and compatible with the purpose for which it was orginally collected?** *Should a responsible party wish to further process peronal information for a compatible purpose, consent is not required from the data subject.*
- **Section 15 of POPIA:** To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of:
  1. the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
  2. the nature of the information concerned;
  3. the consequences of the intended further processing for the data subject;
  4. the manner in which the information has been collected; and
  5. any contractual rights and obligations between the parties.

5 **INFORMATION QUALITY:** The responsible party must take reasonable steps to make sure the personal information is complete, accurate, not misleading and is updated.

<u>Questions to ask:</u>

- **How do you ensure that personal information is reliable and accurate at all times?** *By obtaining information directly from the data source, data accuracy is more probable. It is always advisable to validate the personal information as it is being captured. If it is not possible for the data subject to input their own information, or if the information is captured from one format to another (i.e. from a paper form to an IT system, then the information should be sent to the data subject for validation.)*
- **What process do you have in place to allow data subjects to update their information or object to processing?** *When advising data subjects of the information you hold and for what purpose you hold it, they must be given details of how to update their information or object to processing. It is advisable to develop procedures for automatically checking the accuracy of information on a regular basis, by sending a validation request to the data subjects.*

6 **OPENNESS:** The responsible party must take reasonable steps to notify the data subject of certain information, such as: the information being collected; the purpose for which the information is collected; whether the supply of information is voluntary or mandatory; the consequences of failure to provide information; and any particular law that applies. In the event of unauthorised accessing, processing, erasure or deletion of a data subject's personal information, the responsible party must take reasonable steps to notify the data subject and has to notify the Information Regulator of the event.

<u>Questions to ask:</u>

- **How do you inform the data subject of the purpose for which the information is being gathered?** *The data subject must be informed of how the data will be used at the time of gathering the information.*
- **Does the data subject know who the information officer is?** *When gathering information, data subjects must be given the details of the information officer in your fund, including contact details.*
- **How do you inform the data subjects of their right to lodge a complaint with the Information Regulator?** *At the time that the personal information is gathered, the data subject must be advised of his/her rights to complain to the Information Regulator if misuse is suspected. The Information Regulator's information and contact details must be provided to the data subject.*
- **Have you advised the data subject of his/her rights to access his/her information and to object to the processing of said information?** *This is a requirement.*

7 **SECURITY SAFEGUARDS:** The responsible party must have measures in place to protect the personal information collected and processed from damage, loss and unauthorised destruction, processing and access.

Section 19 of POPIA sets out security measures on integrity and confidentiality of personal information:

1. In order to give effect to subsection (1), the responsible party must take reasonable measures to—
   a. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

b. establish and maintain appropriate safeguards against the risks identified;
c. regularly verify that the safeguards are effectively implemented; and
d. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

2. The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Therefore, a retirement fund must consider the following, among other things, in order to protect the personal information of members:

- Conducting a risk assessment that identifies any foreseeable internal and external risks to personal information in its possession or under its control.
- Establish and maintain appropriate safeguards against the risks identified.
- Implementing measures to prevent personal information from falling into the wrong hands.
- Determining which employees are permitted to access personal information, and what information they are permitted to access.
- Having processes in place to alert the fund when personal information is accessed or modified without authorisation.
- Having processes in place to identify the source of a data breach and the procedure to neutralise such a breach.
- Ensure that safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- Ensure that measures are in place to prevent the reoccurrence of a data breach.

Questions to ask:

What procedure is to be followed when sharing personal information with an operator? *A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator establishes and maintains the required security measures. The operator must advise immediately if there is the possibility that personal data has been accessed or acquired by any unauthorised person.*

What procedure is in place to inform the data subject that their personal information has been compromised? *The data subject must be advised via e-mail or in writing by the responsible party immediately if it is suspected that their personal information has been accessed by unauthorised persons. Sufficient information must be provided to allow the data subject to put measures in place to safeguard themselves against potential consequences of the security compromise.*

What procedure is in place to inform the Information Regulator of any security breach? *The Information Regulator must be informed by the responsible party in the event of a security breach where personal information could be compromised. It is the duty of the responsible party to ensure this is done.*

8

DATA SUBJECT PARTICIPATION: Data subjects can ask what personal information is held about them and can ask for access and changes to their personal information, as well as object to processing.

Questions to ask:

- **What are the data subject's rights regarding access to information being held by you?** *Data subjects may request information from you on whether you are holding their personal information. This request may not be declined and may not be charged for. The full nature and details of the information being held must also be provided on request but a charge may be levied for this information.*
- **What processes do you have in place to ensure such a request from a data subject is adhered to?** *It is the duty of the responsible party to ensure this process is followed.*
- **What processes do you have in place to allow data subjects to correct personal information that you hold or object to the processing of such information?** *The data subject has the right to correct the personal information that you hold. They also have the right to object to processing at any time.*

INFORMATION OFFICERS

Information Regulator

Information officer

Every responsible party has an information officer. Many hold the view (based on legislation) that the default information officer of a retirement fund is the fund's principal officer. The information officer can appoint deputy information officers, but remains responsible for his/her statutory obligations. Information officers and deputy information officers must receive appropriate training and keep abreast of the latest developments in POPIA and the Promotion of Access to Information Act (PAIA).

Duties of the information officer

- **To facilitate retirement fund compliance with the eight principles,** e.g. an information officer should develop a policy on how employees should implement the eight principles.
- **Dealing with, among other things, the various requests that can be made to the retirement fund pursuant to POPIA.** Internal measures are developed together with adequate systems to process requests for or access to information.
- **Working with the Information Regulator in relation to investigations** in relation to the retirement fund (including prior authorisations).
- **A personal information impact assessment** is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
- **A compliance framework** is developed, implemented, monitored and maintained; and
- **Internal awareness sessions** are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Information Regulator.

AT A GLANCE

As responsible parties, retirement funds need to ensure the following actions are taken to be compliant with POPIA on an ongoing basis:

1) There must be a written contract between the responsible party and all identified operators (i.e., certain service providers) to, among other things, ensure that the operator/s establishes and maintains security measures (s19); and

2) In terms of S5(a)(i) members must be notified that their personal information is being collected. The member (data subject) has the right to be aware of:

a. the information being collected and where the information is not collected from the data subject, the source from which it is collected;
b. the name and address of the responsible party;
c. the purpose for which the information is being collected;
d. whether or not the supply of the information by that data subject is voluntary or mandatory;
e. the consequences of failure to provide the information;
f. any particular law authorising or requiring the collection of the information.

3) S19 states that the responsible party must review and implement security measures to:

a. Secure integrity and confidentiality of the personal information
b. Take appropriate, reasonable, technical and organisational measures to:
   i) assess risks
   ii) implement safeguards
   iii) test and update

4) Register and authorise (where required) an information officer.

REFERENCES

- **ASISA**. *ASISA guidelines for responsible parties on the protection of personal information act, 2013.* [Online.] Available at: https://tinyurl.com/taahtsxf
- Axiomatic Insights. [Online.] Available at: https://tinyurl.com/32sbxrcp
- **Information regulator (South Africa)**. Guidance note on information officers and deputy information officers. [Online.] Available at: https://tinyurl.com/5ykv7xm5
- **Institute of Retirement Funds Africa**
- POPI Act Compliance. [Online.] Available at: https://tinyurl.com/dxdwam8n

LEARN MORE

To learn more about this topic, please visit our website www.atleha-edu.org or contact us on 021 851 0091 to find out more about our educational workshops and events.

DEMONSTRATING POPIA COMPLIANCE AND THE RISK OF NON-COMPLIANCE

overview

Complying with POPIA is something all retirement funds need to do, but it is not always clear how POPIA compliance should be achieved. This article looks at some practical ways that retirement funds and their trustees can ensure compliance with the Act.

In the natural course of business, retirement funds are required to process fund members' personal information. This member information will likely include their employment and financial history, their ID numbers and residential addresses, as well as the personal information of their nominated beneficiaries, many of whom are minors. This information is sometimes also processed by the service providers the funds hire to assist with fund administration etc. With the increase in the prevalence of cybercrimes, it is now more important than ever for retirement funds to ensure their compliance with POPIA and to keep members' personal information secure from cybercriminals.

Additionally, under the Protection of Personal Information Act (POPIA), retirement fund trustees are obligated to process personal information in accordance with the conditions for lawful processing. It is very important for retirement funds to comply with POPIA, as there are serious ramifications for trustees that do not comply.

In order for the processing of personal information to be lawful, the following POPIA conditions need to be met:

- **The personal information needs to be collected directly from the data subject.** The "data subject" is a living, natural person (in the case of retirement funds, this could be either the member, trustee or beneficiary of the fund).
- **The information collected needs to be limited to what is required for the required purpose.** This means that the fund cannot request information from members that goes beyond what is absolutely necessary in fulfilling its duties.
- **Purpose specification.** Members need to be informed about the specific reason their personal information is being collected.
- **Information collected must be complete, accurate and up to date.** This is to ensure that the information processed is able to fulfil its purpose and is not misleading in any way.
- **Disclosure to data subject on request.** This means that members can request their fund to disclose what personal information it has about them on record, as well as how the fund is using or intends to use that information.

The caveat to this processing of information is that the fund needs to do what is reasonably practicable. For instance, it is not always practically possible to collect personal information directly from individual members as contacting each individual member will require substantial resources in both labour and time. In this instance, it may be more practical to obtain the information from the member's employer, following POPIA requirements when receiving data from third parties.

Compliance

In the example of processing the personal information of retirement fund members, the board of trustees, which is considered the responsible party, would hire an administrator to perform certain duties, such as paying members their benefits when they retire or exit the fund. In order to fulfil this responsibility, the administrators would need access to members' personal information. POPIA allows for administrators to process members' personal information under two very important conditions:

- All processing of personal information needs to be with the knowledge and authorisation of the board of trustees (who are the "responsible party"); and
- The administrators, who are processing the information on behalf of the responsible party, must consider the information as confidential and cannot disclose it unless required to do so by law.

In this case, both the trustees and their administrator are bound by POPIA. However, it is the responsibility of the board of trustees as the responsible party to ensure that all POPIA conditions for processing information are met as described above. In the event of a contravention of these conditions, it is the retirement fund that will be held liable and not the administrator.

A practical step that trustees can take in order to ensure that they do not become non-compliant to POPIA as a result of actions by their service providers is to draw up a contract with service providers specifying the two conditions stated above. This simple action will ensure that the administrators establish and maintain POPIA-compliant processes and measures needed to keep personal information secure.

It is also important for retirement funds to notify members that they are processing their personal information. Most funds make use of their fund rules, member benefit statements or their annual reports to members to communicate these notices. Whatever the form of communication the fund chooses, the trustees must ensure that the communication includes the following information:

- A description of the information that is being collected, as well as where the information is being collected from should this information not come directly from members.
- The name and address of the responsible party (the fund), as well as the information officer of the fund.
- The reason the information is being collected, as well as the consequences of not receiving the requested information.
- Information on whether disclosing the information is voluntary or mandatory, as well as any laws that authorise the collection of the information if applicable.
- The intention, if applicable, to transfer the information overseas or to an international organisation, as well as the level of protection that will be given to the information by that international organisation.
- Notification of the individual's right to access and rectify the information being processed, the right to object to the processing of their personal information, as well as the right to lodge a complaint with the Information Regulator, for which the contact details of the Regulator also need to be provided.

Codes of conduct

The legal and technical committee of the Institute of Retirement Funds Africa (IRFA) made a number of submissions to the Information Regulator pertaining to retirement funds' processing of personal information. These proposals were potentially to form the basis of a code of conduct for retirement funds and appeals to designate principal officers as information officers under POPIA. These were all in an effort to make it easier for retirement funds to process their members' personal information.

The table below shows a sample extract from the IRFA's code of conduct submitted to the Information Regulator. This submission sought to recognise that retirement funds can process members' personal information without obtaining their consent as well as without obtaining information directly from individual members. As shown below, the extract names the provider and receiver of the personal information, the type of information obtained as well as the legislation that allows for this process to occur.

It is important to note that IRFA is unlikely to propose a code of conduct for retirement funds as, among other things, it does not have the infrastructure to manage a code as required by POPIA and the Information Regulator.

Provider of personal information	Receiver of personal information	Type of information	Law that imposes obligation/ legitimate interest
Fund/ administrator	Fund's auditor Fund's valuator/ actuary Administrator's auditor	Proper registers, books and records of the operations of the fund Including: membership records with details and dates of joining and leaving the fund; contributions received, premiums paid in respect of insured benefits (e.g. death and ill health); payments of pensions and benefits; movement of assets in respect of transfers in and out; payments made to a member leaving the fund other than transfer.	Section 7D(1)(a) Pension Funds Act, 1956 Circular PF No.98

Penalties and fines

As mentioned above, there are costs to non-compliance with POPIA. Retirement funds can be charged hefty fines of up to R10m for non-compliance and some transgressors may even face prison time of up to 10 years. And this is not limited to retirement funds – trustees can also be held personally liable for non-compliance.

The fines, known as administrative fines, are charged to the responsible party if they are found to be in contravention of specific aspects of POPIA. The possible imprisonment of infringers is applicable only to those who in any way hinder the regulator from fulfilling its duties or those who do not respond to a summons or pay their fines; among other offences.

REFERENCES

- **POPIA. 2021.** *Protection of Personal Information Act (POPI Act) – POPIA*. Available at: https://popia.co.za/
- **Michalsons. 2021.** *POPI and pension funds*. Available at: https://tinyurl.com/3rzm9r53
- **Pensionlawyers.co.za. 2021**. Available at: https://tinyurl.com/rkye5eaa

LEARN MORE

To learn more about this topic, please visit our website www.atleha-edu.org or contact us on 021 851 0091 to find out more about our educational workshops and events.

FURTHER RESOURCES ON PERSONAL INFORMATION AND DATA PROTECTION

overview

South Africa's POPIA legislation is not unique. As data breaches have been on the rise globally, legislation has been put in place in other countries and blocs – such as the EU. This article shares some further resources to help position the importance of legislation, such as POPIA, in protecting the personal information of consumers.

1 European Union's General Data Protection Regulation (GDPR), 2018

The General Data Protection Regulation (GDPR) is a European Union (EU) law implemented in May 2018, requiring organisations to safeguard personal data and uphold the privacy rights of anyone in EU territory. The regulation includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated. The GDPR, passed in the European Parliament unifies the EU under a single data protection regime.

GDPR imposes obligations onto organisations anywhere, so long as they target or collect data related to people in the EU. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. With the GDPR, Europe is signalling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence.

Much like POPIA, organisations can comply with the GDPR by implementing technical and operational safeguards to protect and safeguard the personal data they control. The first step is to conduct a GDPR assessment to determine what personal data they control, where it is located, and how it is secured. They must also adhere to the privacy principles outlined in the GDPR, such as obtaining consent and ensuring data portability. Organisations under GDPR regulations may also be required to appoint a Data Protection Officer and update their privacy notice, among other organisational measures. Since GDPR's launch in May 2018, GDPR regulators have issued hundreds of fines to companies, including Google and Facebook, totalling more than €114m.

2 OECD Digital Economy Outlook, 2020

With the rapid emergence of data-rich technologies such as artificial intelligence (AI), the Internet of Things (IoT) and big data analytics, it is increasingly clear that trust remains a critical factor in the digital transformation of economies and societies. Individuals and organisations must feel confident their privacy is respected to take advantage of the benefits arising from technological developments. However, fuelled by high-profile data breaches such as in Cambridge Analytica, individuals are increasingly concerned about digital risks. This is particularly true with respect to the expanded uses of their personal data.

Technological advancement goes hand in hand with increased global data flows. Data has become more valuable (and "big data" especially so), thus increasing incentives to share data, including across borders. Moreover, it is increasingly faster and cheaper to do so. However, as the quantity of data collected and stored increases, so too does the prevalence of data breaches. Such breaches can result from accidents, malicious hacking, unauthorised access or disclosure, phishing and denial-of-service attacks.

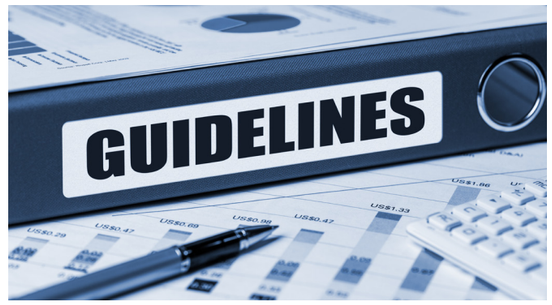
Between 2018 and 2019, over 89 000 data breaches were registered in the EU, representing an increase of 20% from 2015. It is likely, however, that the GDPR's mandatory data breach reporting requirement contributed to this substantial increase.

In recent years, the private sector has been involved in high-profile data breaches. In October 2018, Facebook was fined £500 000, the maximum fine possible by the Information Commissioner's Office of the United Kingdom. It was charged for "unfairly processing personal data" and "failing to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data". The incident involved more than 87 million personal records that were unlawfully used by Cambridge Analytica.

Data breaches, however, are not limited to data held by the private sector. In 2015, for example, more than 21 million records stored by the US Office of Personnel Management were stolen, including 5.6 million fingerprints. In the same year, a breach in the Japanese Pension Service affected 1.25 million people.

Data breaches violate the privacy of individuals concerned (leading possibly to identity theft), and can also cause significant economic losses to affected organisations. The increasing prevalence and cost of data breaches have contributed to changing public awareness and perceptions of the importance of privacy.

The OECD is therefore currently reviewing the implementation of the 2013 revisions to the 1980 OECD Privacy Guidelines. The guidelines are intended as minimum standards for adoption in domestic legislation regarding the protection of personal data, and have influenced legislation and policy in OECD countries and beyond. The current review aims to monitor implementation of the 2013 guidelines, identify gaps and suggest possible next steps to ensure the OECD's Privacy Guidelines remain relevant.



3 Guidelines for ASISA members on the POPI Act of 2013, 2021

In July 2021, ASISA published Guidelines for ASISA members on the POPI Act of 2013. In seeking to comply with POPIA, ASISA members developed the guidelines as general principles to assist ASISA members in implementing POPIA.

The main objective of the guidelines is to promote high standards of behaviour and provide for, as practically as possible, a consistent approach on the part of ASISA members in their efforts to address their handling of personal information – as envisioned in POPIA and by the Information Regulator.

The guidance notes and examples provided within the guidelines are included to provide general guidance to ASISA member organisations in respect of the application and interpretation of POPIA, but are not prescriptive and have no binding legal force and effect.

Although the guidelines set out standards of good practices relating to the processing of personal information and are intended to guarantee a uniform, high-level of information protection, individual ASISA member organisations must always ensure that they are compliant with the provisions of POPIA and/or any documents and guidance notes published by the Information Regulator. In the event of any discrepancy or inconsistency between the ASISA Guidelines and POPIA, POPIA will prevail.

The guidelines aim to:

- Provide ASISA members with principles which they should endeavour to meet in their dealings with data subjects and the processing of their personal information;
- Provide information to data subjects whose personal information is (or will be) processed by ASISA members; and
- Contribute to the transparency of the principles applied in respect of the personal information processed and to be processed by ASISA members.

REFERENCES

- **ASISA.** *ASISA guidelines for responsible parties on the protection of personal information act, 2013.* [Online.] Available at: https://tinyurl.com/taahtsxf
- GDPR website: https://gdpr.eu/
- OECD (2013), ***OECD Privacy Framework***, OECD Publishing, Paris, https://tinyurl.com/nvdrvpd5
- OECD (2020), ***OECD Digital Economy Outlook 2020***, OECD Publishing, Paris, https://tinyurl.com/mzwcftk6

LEARN MORE

To learn more about this topic, please visit our website www.atleha-edu.org or contact us on 021 851 0091 to find out more about our educational workshops and events.

ASISA ACADEMY ASISA FOUNDATION

RETIREMENT FUND TRUSTEE EDUCATION WORKSHOPS

PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

The **ASISA Academy**, in partnership with the **ASISA Foundation**, offers a fully-funded, independently delivered workshop for South African retirement fund principal officers and trustees in order to provide delegates with an in-depth understanding of the **Protection of Personal Information Act** (POPIA).

The **POPIA workshop** is delivered online and it promotes the protection of personal information processed by public and private bodies. It also seeks to balance the right to privacy against other rights, such as access to information.

THE WORKSHOP'S 5 LEARNING AREAS INCLUDE

1. ORIGINS AND OBJECTIVES OF THE LEGISLATION
2. DEFINITIONS
3. CONDITIONS
4. GOVERNANCE IMPLICATIONS FOR RETIREMENT FUNDS
5. TIMELINES FOR IMPLEMENTATION

Comments from previous workshop participants:

"I found the entire presentation, theoretical knowledge and the flow of the presentation useful and relevant."

"The workshop was excellent, thank you."

ASISA ACADEMY

Accredited CPD provider for the Batseta Council for Retirement Funds.

FOR MORE INFO CONTACT:
LEARN@asisaacademy.org.za

USE THE LINK BELOW TO REGISTER FOR THIS WORKSHOP
https://tinyurl.com/pc2b6dhr

Batseta 2021 CPD Provider

REGISTER FOR CPD CREDITS THROUGH ATLEHA-EDU'S CONSUMER EDUCATION

Atleha-edu's initiatives are accredited in partnership with the Batseta Council of Retirement Funds for South Africa. To register your interest in being awarded Continuous Professional Development (CPD) credits for having read this publication, please provide the required details below:

First name/s: _____ **Surname:** _____

South African ID number: _____ **Postal address:** _____

Demographic profile:
(Required for FSC Consumer Education Compliance)

- ☐ African
- ☐ Coloured
- ☐ Indian
- ☐ White
- ☐ Other

Designation:
(Please tick only the appropriate box)

Trustee
- ☐ Employer nominated
- ☐ Employee nominated
- ☐ Independent trustee

- **Principal officer** ☐
- **MANCO member** ☐

Name of retirement fund/s:

Fund 1 _____

Fund 2 _____

Fund 3 _____

Email address: _____ **Cellphone number:** _____

Alternative email address: _____ **Alternative phone number:** _____

☐ **Please update my details per the above information provided and send me** Atleha-edu's **complimentary educational publications via email**

Please return this completed form to:
Email: cpd@atleha-edu.org
Postal: Atleha-edu, Postnet Suite 272, Private Bag, Somerset West, 7129

Batseta
2021 CPD Provider

TEST YOUR LEARNING TO RECEIVE CPD CREDITS

Atleha.edu Consumer Financial Education initiatives are accredited for Continuous Professional Development (CPD) in partnership with the Batseta Council of Retirement Funds for South Africa.

To register your CPD credits for having read this Atleha-edu Consumer Education publication, please complete the following quiz and return this completed form via email to: cpd@atleha-edu.org or post it to: Atleha-edu, Postnet Suite 272, Private Bag, Somerset West, 7129

Example question: Please choose the correct answer.

True or false? As of 1 July 2021, the Protection of Personal Information Act (POPIA) largely came into effect.

- [x] True
- [ ] False

1. Choose the correct answers. Which of the following are probably data subjects as defined by POPIA?

- [ ] Fund members
- [ ] Fund administrator
- [ ] Spouse of a member
- [ ] Pensioners

2.True or false? The Information Regulator must be informed in the event of a security breach where personal information has been compromised.

- [ ] True
- [ ] False

3. Choose the correct answer. What is the second general protection principle under POPIA?

- [ ] Purpose specification
- [ ] Openness
- [ ] Processing limitation
- [ ] Security safeguards

4. Fill in the missing words. The _____ is the public/private body that processes personal information.

5. Choose the correct answer. An additional measure to ward off cyberattacks is assuming that every facet of an organisation is compromised and setting up precautions to validate every user, device and connection into the organisation for authenticity and for purpose. This is known as:

- [ ] Cloud security
- [ ] Network security
- [ ] A zero-trust security strategy
- [ ] Information security

6. Choose the correct answer. Failure to comply with POPIA can see retirement funds fined by up to a maximum of:

- [ ] R1 million
- [ ] R5 million
- [ ] R10 million
- [ ] R15 million

6.True or false? Subject to a number of exceptions (or justifications), personal information must be collected directly from the data subject themselves.

- [ ] True
- [ ] False

8. Fill in the missing words. Under POPIA, a retirement fund's _____ is the default information officer.

9. Which of the following is NOT the Information Regulator's duty in terms of POPIA compliance and regulation?

- [ ] Monitoring and enforcing compliance
- [ ] Developing a compliance framework for responsible parties
- [ ] Handling of complaints
- [ ] Issuing codes of conduct/guidelines

10. Choose the correct answer. Which of the following does **NOT** form part of an information officer's duties under POPIA?

- [ ] Facilitating retirement fund compliance with the eight principles
- [ ] Conducting a personal information impact assessment
- [ ] Ensuring a compliance framework is developed, implemented, monitored and maintained
- [ ] Monitoring and enforcing private and public sector POPIA compliance