

PRACTICAL IMPLEMENTATION OF THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA) at Glacier by Sanlam

Upholding our clients' constitutional right to privacy.



glacier
by Sanlam

We are all data subjects. From the moment you are born, you have personal information that is processed by someone, somewhere. The Protection of Personal Information Act, 2013, commonly known as POPIA, is there to ensure that every South African citizen's constitutional right to privacy is upheld through the protection of their personal information.



WHAT IS POPIA?

In essence, POPIA gives effect to section 14 of the Constitution which provides that everyone has the right to privacy. It provides the regulatory framework within which responsible parties may process personal information of data subjects (both natural persons as well as juristic persons).

Role-players related to POPIA

- **Data subject:** Data subjects are the people to whom the personal information (PI) that is being processed relates.
- **A responsible party (RP)** refers to a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing. Simply put, this means the RP determines what PI is required, the how and why for the processing of PI.
- **Operators (Ops):** In serving its customers, a RP may contract another party, known as operators (OPs) to process PI on their behalf. The OP is a natural or juristic person who processes PI for a RP, in terms of a contract, without coming under the direct authority of the RP.
- **The Information Regulator (IR)** refers to a body that was set up to govern all conditions of the lawful processing of personal information in terms of both the Protection of Personal Information Act, 2013 (POPIA) and Promotion of Access to Information Act, 2000 (PAIA). These Acts grant the Information Regulator many powers. These include requiring Responsible Parties to register Information Officers and powers to inspect the implementation of POPIA at a Responsible Party which may result in enforcement actions. Under certain conditions, the Responsible Party must report POPIA breaches to the Information Regulator
- **Information Officer (IO):** The Information Officer (IO) is responsible for governance in all RP contexts. The Information Officer has to ensure compliance to all relevant requirements and conditions of the relevant legislation. The IO has to be registered, via the government portal, by the end of June 2021. The regulator will direct all correspondence and queries to the Information Officer.
- **Deputy Information Officers (DIOs):** In a large company, IOs may appoint Deputy Information Officers (DIOs) to help carry out some of the duties of the IO.

WHAT IS PERSONAL INFORMATION?

“Personal information” refers to **information relating to an identifiable, living natural person (and, where applicable, a juristic person)**, including gender, marital status, age, identity number, email address, telephone number and physical address.

The act also makes provision for “special personal information”, which is information of a more sensitive nature, such as information concerning children, religious affiliation, race or ethnic background, trade union membership, political affiliation, medical and genetic information and criminal records.

WHAT DOES PROCESSING MEAN?

Processing refers to all of the activities that could relate to handling PI – including, but not limited to, collection, receipt, collation, storage, updating, retrieval, use, destruction and the alteration or distribution of a record which contains PI.

If you process any PI (for example ID numbers, contact or bank details, etc.) or documents containing PI, whether the information relates to your employees, clients, or suppliers, you act in the capacity of a responsible party.

Personal information must be processed:

- lawfully; and
- in a reasonable manner that does not infringe on the privacy of the data subject.

Section 10 stresses this point: it states that personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive. Put differently: the responsible party should only process the minimum information they need to adequately fulfil the purpose for which it is being used.

In order for processing to be “lawful” it must comply with the minimum requirements as set out in the legislation. There are eight conditions for lawful processing.

1. **Accountability** – as a responsible party (RP), you’re accountable for compliance with POPIA.
2. **Processing limitation** – you may only process the minimum information needed to fulfill the purpose for which the PI was collected. In essence, the personal information being processed must tie up with the purpose for which it was obtained. Responsible parties may not process data which goes over and above the stated purpose.
3. **Purpose specification** – PI must be collected for a specific, explicitly defined and lawful purpose related to the responsible party’s function or activity.
4. **Further processing limitation** – further processing of PI must be compatible with the original purpose of collection of the PI.
5. **Information quality** – the RP must take reasonably practical steps to ensure the PI is complete, accurate, not misleading and up-to-date, having regard to the purpose for which the PI is collected or further processed.
6. **Openness** – you have to be transparent about your reasons for obtaining PI and ensure that what you do with the information is in line with the reasonable expectations of the data subject.
7. **Security safeguards** – you must secure the integrity and confidentiality of PI by taking appropriate, reasonable, technical and organisational measures to prevent loss, damage, unauthorised destruction of, and unlawful access to, or processing of PI.
8. **Data subject participation** – the data subject has the right to request you to confirm what PI you hold and with whom you have shared it, as well as to request you to correct, update or delete their PI.

RULES AROUND THE RETENTION OF RECORDS

You may not retain records of PI for longer than is necessary for achieving your purpose for collecting the information, unless:

- retaining the record is required or authorised by law (for example, FAIS requires records to be kept for five years after termination); or
- the responsible party needs the record for lawful purposes related to its functions or activities (*for example, where a product provider needs to keep personal information about a customer so that they can deal with possible complaints about the services or to defend possible future legal claims); or
- retaining the record is required by a contract between the parties; or
- the data subject (or a competent person where the data subject is a child) has consented to you retaining the record.

If you retain the records, you must establish appropriate safeguards against the PI being used for any other purpose.

BREACH OF PERSONAL INFORMATION

PI has become a currency for cyber criminals. Hacking and cyber attempts to access PI have become commonplace and even seemingly secure systems have borne the brunt of this criminal activity. Therefore, it has become incumbent on all responsible parties to ensure that PI is handled with due care and integrity, and to employ every possible means to ensure that PI is adequately protected.

CONSEQUENCES OF NON-COMPLIANCE

Non-compliance with POPIA can result in legal action, administrative fines and even jail time. In addition, the resultant reputational and brand damage couldn't be quantified. And not to mention the trust relationship that would be broken between you and the data subject, your client.



PRACTICAL IMPLEMENTATION AT GLACIER

With due regard for this legislation, Glacier has added POPIA-related disclosures to our forms and other relevant documentation, as well as to our systems and websites.

These disclosures also contain a link to our privacy policy at www.sanlam.com/legal/Pages/sanlams-privacy-policy.aspx to make sure data subjects are informed of how we collect personal information, what personal information we collect, how we use that information, who we will share that information with, how we protect personal information, etc. We also share the Information Regulator's contact details in our privacy policy.



Popia disclosure added to online systems, documents and forms

As per Section 18 of POPIA, a data subject needs to be notified (made aware) of Glacier's Privacy Policy before we collect (capture) personal information. We have therefore made changes to ensure that clients are notified of this.

1. POPIA disclosure added to Investment Hub, Life Annuities and Investments Quote System (LAIQS), ICE, Intermediary web and Client web

On the **Investment Hub**, we have included a static message to remind you that you need to make your clients aware of Glacier's Privacy Policy:

You are about to provide Glacier with personal information. Please ensure your client is familiar with our Privacy Policy. By continuing, you confirm that you made your client aware of why we need their personal information, what we do with it, as well as their rights. **Read more ...**

It will show on the following pages:

- New client
- Client summary
- Import Client
- New investment case

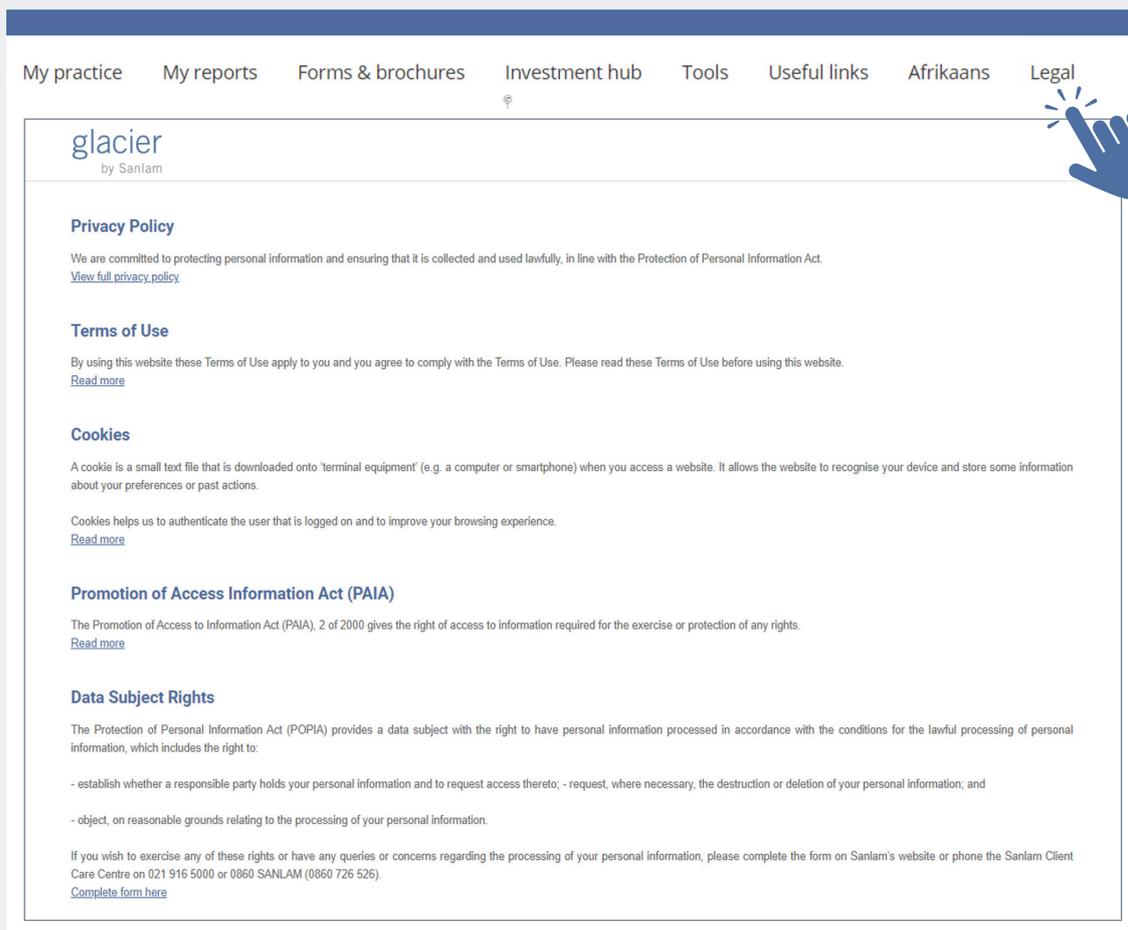
On the **Life Annuities and Investments Quote System (LAIQS)** and **ICE tool**, the same message was added to the *Client* page.

On the **Intermediary web & the Client web**, the message was added to the *Client details* page.

2. Legal page added on the intermediary web, client web, Investment Hub, and Life Annuities and Investments Quote System (LAIQS)

Glacier has created a specific Legal web page, which has been updated with all the relevant POPIA requirements. Links are provided to access:

- our privacy policy,
- the terms of use of the website,
- the cookies policy,
- the PAI Manual
- the rights of the data subject



The screenshot shows the Glacier by Sanlam website's Legal page. The navigation menu includes 'My practice', 'My reports', 'Forms & brochures', 'Investment hub', 'Tools', 'Useful links', 'Afrikaans', and 'Legal'. The 'Legal' link is highlighted with a hand icon. The page content includes the following sections:

- Privacy Policy**: We are committed to protecting personal information and ensuring that it is collected and used lawfully, in line with the Protection of Personal Information Act. [View full privacy policy](#)
- Terms of Use**: By using this website these Terms of Use apply to you and you agree to comply with the Terms of Use. Please read these Terms of Use before using this website. [Read more](#)
- Cookies**: A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when you access a website. It allows the website to recognise your device and store some information about your preferences or past actions. Cookies helps us to authenticate the user that is logged on and to improve your browsing experience. [Read more](#)
- Promotion of Access Information Act (PAIA)**: The Promotion of Access to Information Act (PAIA), 2 of 2000 gives the right of access to information required for the exercise or protection of any rights. [Read more](#)
- Data Subject Rights**: The Protection of Personal Information Act (POPIA) provides a data subject with the right to have personal information processed in accordance with the conditions for the lawful processing of personal information, which includes the right to:
 - establish whether a responsible party holds your personal information and to request access thereto; - request, where necessary, the destruction or deletion of your personal information; and
 - object, on reasonable grounds relating to the processing of your personal information.

If you wish to exercise any of these rights or have any queries or concerns regarding the processing of your personal information, please complete the form on Sanlam's website or phone the Sanlam Client Care Centre on 021 916 5000 or 0860 SANLAM (0860 726 526). [Complete form here](#)

3. Legal links: Websites including mobile website

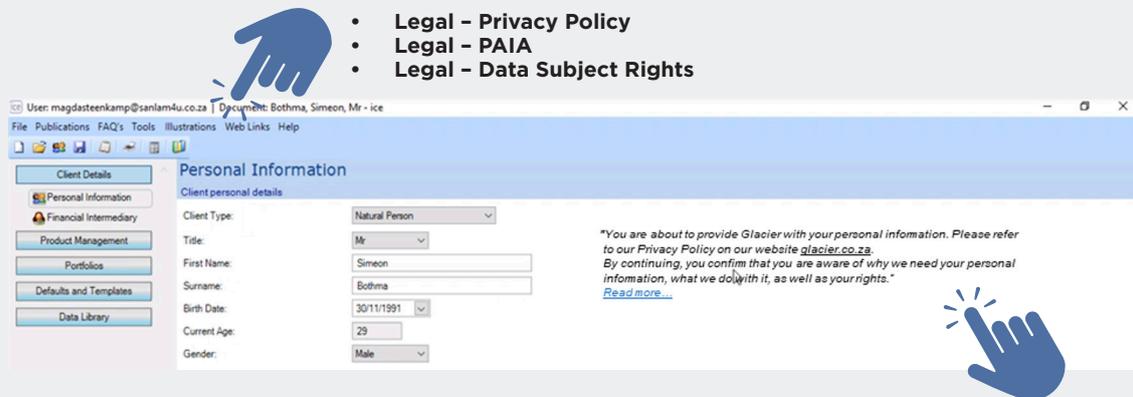
On **our websites**, in the existing *Legal* section at the bottom of the page, a link to *Data Subject Rights* has been added.

The **mobile website** has been updated with links to:

- our privacy policy,
- the terms of use of the mobile site,
- the rights of the data subject

These will be displayed in the footer of the website.

In the **ICE tool**, the *Web Links* menu item at the top will also link to the privacy policy, PAIA and data subject rights:



- **Legal - Privacy Policy**
- **Legal - PAIA**
- **Legal - Data Subject Rights**

The screenshot shows a web browser window with the URL `http://www.sanlam4u.co.za`. The browser's menu bar includes 'File', 'Publications', 'FAQ's', 'Tools', 'Illustrations', 'Web Links', and 'Help'. The main content area is titled 'Personal Information' and contains a form for 'Client personal details'. The form fields include: Client Type (Natural Person), Title (Mr), First Name (Simeon), Surname (Bothma), Birth Date (30/11/1991), Current Age (29), and Gender (Male). To the right of the form, there is a privacy notice: *"You are about to provide Glacier with your personal information. Please refer to our Privacy Policy on our website glacier.co.za. By continuing, you confirm that you are aware of why we need your personal information, what we do with it, as well as your rights."* with a [Read more...](#) link. A blue hand icon points to this notice.

4. New “How we protect your personal information” section on forms and other documentation

A *How we protect your personal information* section was added to the terms and conditions on the application forms, as well as to quotes, client detail & third party maintenance forms, investment confirmations, and client statements.

We also included the Information Regulator’s details on the Investment confirmations.

4.1 Application forms terms and conditions

A section was added to the terms and conditions on our application forms to inform the client of the following:

- Who they are sharing their information with
- What we collect and how we collect it
- Who we share their personal information with
- What we do with their information

4.2 Quotes

A section has been added to explain how we protect personal information, with a link to our privacy policy on the web (www.sanlam.com/legal/Pages/sanlams-privacy-policy.aspx).

4.3 Client detail & third party maintenance forms

This message to explain who we protect personal information, with a link to our privacy policy on the web, is displayed right above where the client signs.

4.4 Investment confirmations

A section was added to the terms and conditions on our application forms to inform the client of the following:

- Who they are sharing their information with
- What we collect and how we collect it
- Who we share their personal information with
- What we do with their information

The contact details of the **Information Regulator** was also added to the Complaints section of investment confirmations.

4.5 Statements (Glacier & Namibia)

The section “Important information notes” was expanded to include information on how we protect personal information, with a link to our privacy policy on the website.

5. Personal Details tab on all statements, investment confirmations and maintenance letters where clients can update personal details (Glacier & Namibia)

A message was added:

You are about to provide Glacier with your personal information. By continuing, you confirm that you understand why we need your personal information, what we do with it, as well as your rights.

For more information, you can access our complete privacy policy at www.sanlam.com/legal/Pages/sanlams-privacy-policy.aspx.

Submit

6. Morningstar

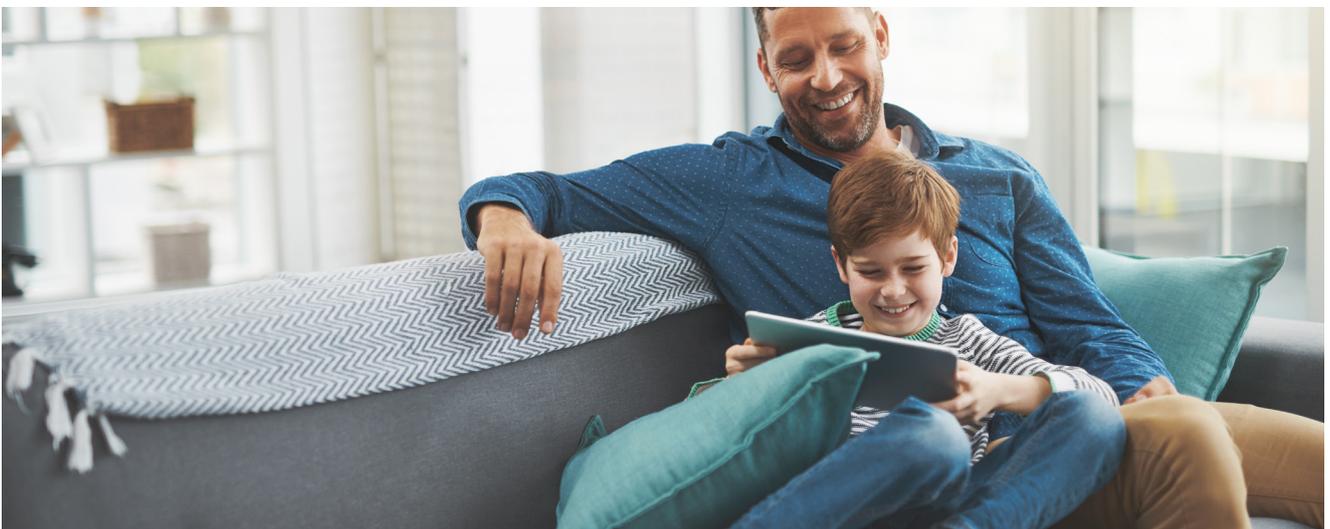
A message was added to the Morningstar deduction authorisation form and the workstation contracts, informing users that they’re about to provide us with their personal information. It contains a link to our privacy policy on the web, and explains to the user that by continuing, they confirm their awareness of why we need their personal information, what we do with it as well as their rights.

7. Website complaints form

A section was added on the website where the complaints form is hosted. It reads as follows:

When you submit this form to us, you are sharing your personal information with us and you confirm that you understand why we need your personal information, what we do with it, as well as your rights.

A link is also provided to our privacy policy.

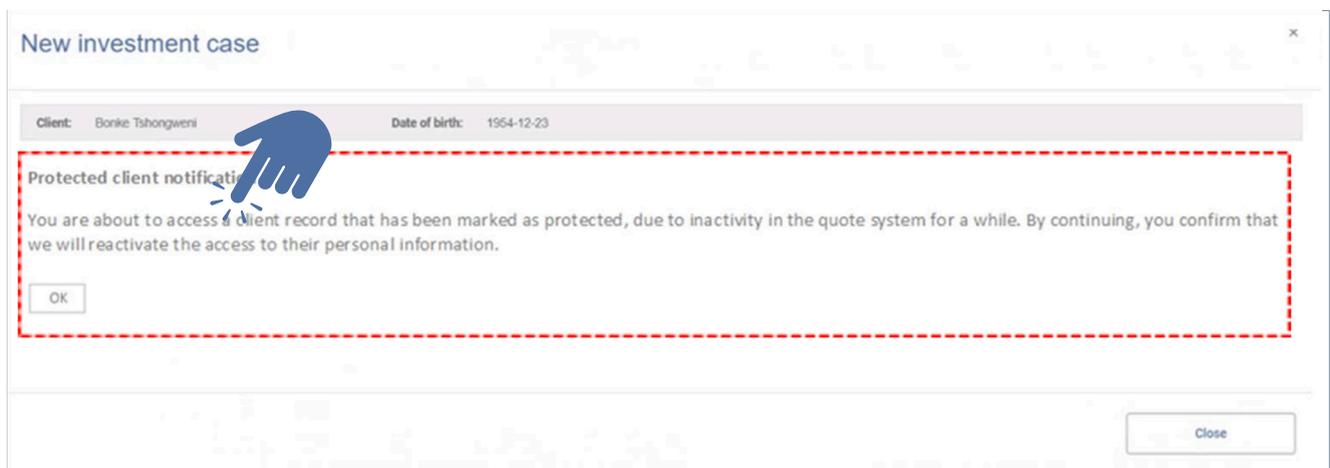


RETENTION OF RECORDS

Glacier has adopted the general responsibility guidelines of the Sanlam Group and we are committed to effectively and lawfully retain our records in accordance with the specified periods. Condition 3 of POPIA provides that records must not be retained for any longer than is necessary to achieve the purpose of collection. However, there are instances where Glacier can justify retaining the records for longer periods.

Within our **quote systems** we have taken steps to restrict and protect the personal client information that was captured, after a year of no activity in that particular system.

However, as we know, clients have long-term relationships with intermediaries and potentially you may need to advise and provide a client with a new quote after a year has passed. **The record can easily be unrestricted by a simple confirmation click of a button.** This confirmation will be stored and referred to if questions arise in the future as to when and why the information was accessed.



On both the Investment Hub and the Life Annuities and Investments Quote System, the message reads as follows:

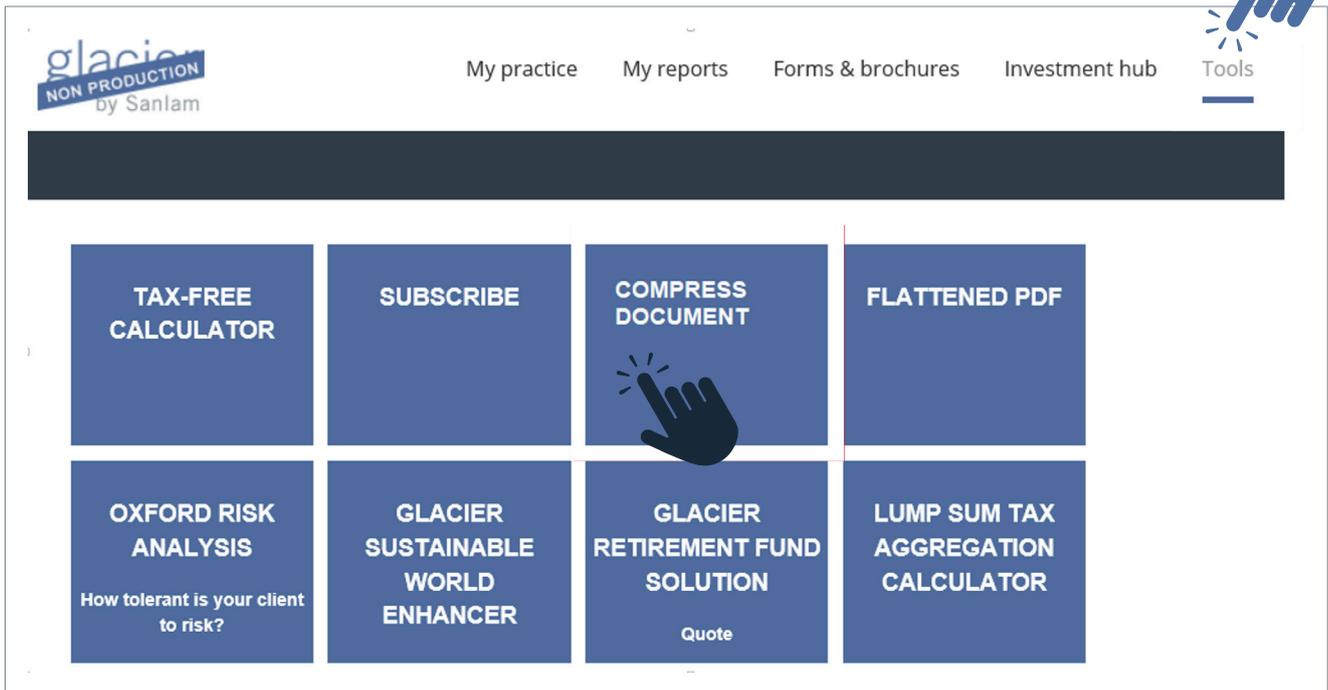
Protected client notification

You are about to access a client record that has been marked as protected, due to inactivity in the quote system for a while. By continuing you confirm that we will reactivate the access to their personal information.

COMPRESSED DOCUMENT TOOL ADDED

Glacier has realised the need to have a POPIA compliant solution to compress large pdf documents when submitting via the Investment Hub or email. Previous solutions like Google converter are not seen as compliant because they save a version on an international server.

There is a new tool on the Tools page of the intermediary web that should be used to compress large pdf documents:



- When the *Compress Document* tile is clicked, the *Compress PDF Document* window will open.
- Click on the 'Browse' button. A window will open for you to select the file on your PC that must be resized.
- Go to the appropriate directory and select the file.
- Click the 'Open' button to select the file for compression:
- The selected file will be displayed below the 'Browse' button.
- Click the 'Compress' button to compress the file. Low compression reduces the size by +- 60%, and high compression reduces the size by +- 90%.
- Once the compression is done a message box will be displayed below the Compress window to ask if you want to save or open the file.
- Click the 'Open' button to view the compressed file. Once the file is open it can be saved as a normal file. Alternatively click the 'Save' button to save the file to a directory on your PC.
- The size of the compressed document will be smaller than the original document and can now be uploaded into the Investment Hub or emailed.

Important: Only documents originally created in pdf can be compressed. Documents that have been converted to pdf will cause an error message to appear when compressing is attempted.

EMAIL AND DOCUMENT ENCRYPTION AND PASSWORD PROTECTION

We have the responsibility to ensure that we take all appropriate precautions to protect personal information (PI) when distributed in the body of an email or any attachment that contains PI.

Much attention has been given to securely transmitting information via email, with some calls being made for all emails and their attachments to be encrypted (or password-protected).

In this regard, the Sanlam group is following an approach that seeks to minimise the impact on our existing business processes without compromising the security of our clients' information. The following is recommended with regard to your email communications with us:

1. Ensure that your email server is set to use TLS (Transport Layer Security). It is the default setting for Microsoft Exchange and other large-scale email servers. This ensures that your emails are secure and safe from access while being transmitted between your server and ours. This is a sufficient level of security for POPIA Data Protection needs.
2. Please don't separately encrypt attachments, because this will mean that the client documents you're submitting cannot be processed automatically. Instead they will need to be decrypted manually by our staff before they can be processed, and this will lead to significant delays in the processing of transactions.



NEW DATA SUBJECT PARTICIPATION PROCESS

As per Section 11, 23 and 24 of POPIA, a data subject (e.g. a Client) has the right to request:

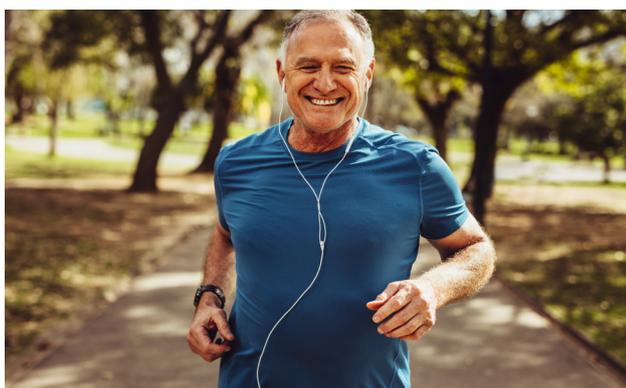
- if we hold any PI of them
- access to the PI we hold of them
- access to some specific PI we hold of them, i.e. a record, detail linked to their PI, third parties that has access to it, PI these third parties hold, etc.
- correction of their PI
- us to stop processing their PI

Clients have to be **referred to** the **Sanlam Client Care Centre** on 021 916 5000 or 0860 SANLAM (0860 726 526) or Sanlam's website (Sanlam.co.za) to complete a **form online**.

As the intermediary, you can also complete the form on the client's behalf.

Important

1. *This process does **not** replace the existing process or policies, such as client maintenance, requesting statements, who is allowed to see what, etc.*
2. *This process should **not** be followed when a client wants to **opt out** of direct marketing.*
3. *Intermediaries should not encourage clients to follow this process unless they have good reason to believe that Glacier is not processing their information lawfully and in line with POPIA. The objective of the process is not a "quick check to see" and it takes about 30 days to receive a response.*
4. *If the requestor is not the data subject, refer to Form C in the PAIA Manual.*



Examples

- A client/potential client **wants to know what** personal information about them, over and above what's on the Member Portal, **is held** across Sanlam.
- A client/potential client believes we have personal information about them that we shouldn't have - they **want to see something specific** (referring to information or a document).
- A client/potential client believes we have personal information about them that is unnecessary/irrelevant - they **want us to delete** it.
- A client/potential client believes we have personal information about them that we obtained or processed unlawfully - they want to know **how and where we got it**.
- After referring a client/potential client to Sanlam's Privacy Policy, they want to know **who we are sharing** their personal information **with specifically**.
- A client/potential client believes we are sharing their personal information with someone we shouldn't - they want us to **stop sharing** it with them.
- After referring a client/potential client to Sanlam's Privacy Policy, they want us to **delete** all their personal information from all Glacier/Sanlam systems.

Important: *If a client/prospective client believes we are not processing their personal information lawfully, using it for something we're not supposed to, or in a manner that infringes on their privacy, they have to lodge a complaint to Glacier/Sanlam.*

NEW PI DATA BREACH PROCESS

As per Section 22 of POPIA, a responsible party (e.g. Sanlam, Glacier, Intermediaries, etc.) has to manage personal information data breaches.

This will be done centrally for Sanlam and includes Glacier. All intermediaries are to follow this process.

A data breach is when personal information is:

- lost, damaged or unlawfully destroyed; or
- accessed, or processed unlawfully.

Intermediaries have to notify Sanlam of data breaches by mailing POPIABreach@Sanlam.co.za, with the following information:

- Location of the incident
- Date and time
- Description of the incident
- The nature of the information
- Details of person reporting incident
- Details of the data subject/s impacted

Important: A data breach includes both confirmed and suspected incidents

Examples of a PI Data Breach

- Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information.
- Unauthorised access to personal information by an employee.
- Inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person.
- Access by an unauthorised third party or unlawful disclosure of personal data to a third party.
- Deliberate or accidental action (or inaction) by a responsible party or operator that compromises the security of personal information.
- Alteration of personal data without permission.
- Loss of availability of personal data, e.g. unauthorised destruction.
- Data input error/human error.
- Non-secure disposal of hardware or paperwork containing personal data.
- Inappropriate access/sharing allowing unauthorised use of, access to or modification of data or information systems.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

NEW 'OPT OUT OF DIRECT MARKETING' PROCESS

As per Section 11 of POPIA, a data subject (e.g., a Client) has the right to:

- object to the processing of their PI for direct marketing
- withdraw consent that was previously given for direct marketing

Clients should be **referred** to the **Sanlam Client Care Centre** on 021 916 5000 or 0860 SANLAM (0860 726 526)

Important: Opting out at Sanlam will mean opting out of direct marketing from the entire Sanlam Group.

Thank you for supporting Glacier's commitment to conducting business lawfully, ethically, and with integrity. Should you have any questions, please contact your Glacier representative.

This document is intended for use by financial intermediaries.

The information in this document is provided for information purposes only and should not be construed as the rendering of advice to clients. Although we have taken reasonable steps to ensure the accuracy of the information, neither Sanlam nor any of its subsidiaries accept any liability whatsoever for any direct, indirect or consequential loss arising from the use of, or reliance in any manner on the information provided in this document.

Glacier Financial Solutions (Pty) Ltd. | A member of the Sanlam Group | Private Bag X5 | Tyger Valley 7536 | Email client.services@glacier.co.za | Tel +27 21 917 9002 / 0860 452 364 | Fax +27 21 947 9210 | Web www.glacier.co.za | Twitter @GlacierBySanlam | Reg No 1999/025360/07 | Licensed Financial Services Provider

Sanlam Life Insurance Ltd. | Email life@sanlam.co.za | Tel + 27 21 916 5000 / 0860 726 526 | Fax +27 21 947 9440 | Reg No 1998/021121/06 | Licensed Financial Services Provider

glacier
by Sanlam