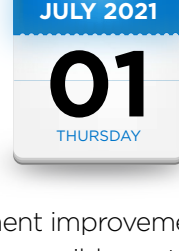


Update on Sanlam Corporate's implementation of the Protection of Personal Information Act, 2013

Sanlam Corporate's road to readiness

The Protection of Personal Information Act 4 of 2013 (POPIA) will come into full effect on 1 July 2021. POPIA gives effect to the right to privacy as set out in the Constitution of the Republic of South Africa and aims to protect the personal information of data subjects by striking a balance between the rights to privacy, access and flow of information.



Sanlam Corporate (Sanlam) has evaluated its systems and processes and continues to implement improvements to ensure that where Sanlam processes the personal information of a data subject as the responsible party or operator, this complies with the requirements of POPIA.

Data Subject
The person to whom the personal information (PI) relates. PI is defined in POPIA and refers to information relating to an identifiable, living natural person or an identifiable, existing juristic person.
<i>Example: Member, employee, etc.</i>

Responsible Party / Joint Responsible Party	Operator
The person/entity determining what and how PI must be processed. This decision may be made alone or in conjunction with another party.	The person/entity processing PI for a responsible party in terms of a contract or mandate but who does not come under the direct authority or control of the responsible party.
<i>Example: Retirement funds, employers, intermediaries, insurer etc.</i>	<i>Example: Third party providers, retirement fund administrators, etc.</i>

The role (as the data subject, responsible party or operator) of a particular person/entity will depend on, amongst other things, the context and the terms of the relevant policy or contract.

Sanlam is the trusted custodian of the personal information of many retirement funds, employers, members, policyholders and clients. Sanlam processes personal information in line with the following eight conditions set out in POPIA:

Accountability:

Sanlam complies with and adheres to POPIA.

Processing Limitation:

Sanlam processes personal information only where a legitimate basis exists, in a fair, lawful, and non-excessive manner.

Purpose Specification:

Sanlam only processes personal information for a specific, explicitly defined and lawful purpose. Records of personal information are not retained any longer than is necessary for achieving this purpose.

Further Processing Limitation:

Sanlam does not process personal information for a secondary purpose unless that secondary purpose is in accordance with or compatible with the original purpose or authorised by POPIA.

Information Quality:

Sanlam makes every reasonable effort to ensure that the personal information processed is complete, accurate, up to date and not misleading. Sanlam relies on other role players to do the same when submitting personal information to Sanlam.

Openness:

Sanlam ensures that data subjects are aware of the processing of their personal information, including the source and purpose of its collection.

Security Safeguards:

The integrity and confidentiality of personal information is protected by taking appropriate, reasonable technical and organisational measures.

Data Subject Participation:

Sanlam ensures that data subjects have access to their personal information (and may request the deletion or correction of their personal information).

Sanlam is committed to:

- Ensuring that all personal information is processed in a responsible manner that does not unjustifiably infringe the privacy of any data subjects.
- Securing the integrity and confidentiality of personal information in our possession or under our control.
- Complying with legislation, including but not limited to data protection laws.

POPIA is very much a principle-based piece of legislation. It seeks to establish a privacy culture as well as minimum requirements to adhere to.

We will continue to communicate regularly with our clients regarding our progress and welcome any questions that you might have. Please direct these through your usual channels.



Will Sanlam Corporate be POPIA compliant by 1 July 2021?

Yes, Sanlam will be compliant with POPIA by the deadline of 1 July 2021.

Will Sanlam Corporate adhere to the eight conditions of lawful processing?

Yes, Sanlam will be compliant with POPIA by the deadline of 1 July 2021. A privacy culture is already embedded in our business and this will be enhanced. Sanlam actively manages compliance to POPIA and its principles and conditions.

What are the legitimate bases on which Sanlam relies in processing personal information?

Sanlam only processes personal information when one of the following legitimate bases applies:

- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied;
- the data subject (or a competent person where the data subject is a child) consents to the processing.

Does Sanlam process special personal information or personal information of children, and if so, what additional measures will Sanlam be taking when processing this information?

Yes, there are instances where we process this type of information in performing our contractual obligations or in accordance with legal and regulatory requirements. Sanlam will only process special personal information where there is a legitimate basis to do so. For example:

- children's information will be processed in respect of insurance cover and beneficiaries, beneficiary nominations, beneficiary fund administration and Section 37C administrative activities; and
- a person's health information will be processed in the administration of insurance underwriting, death, and disability claims.

As this information is processed by function-specific teams and already categorised as sensitive information, significant additional security is already in place for the processing of this information.

Do you store any personal information using cloud storage? If so, what measures have you taken to comply with POPIA?

Yes, Sanlam stores some personal information on cloud storage solutions. Sanlam is constantly enhancing its technology infrastructure to remain sustainable, advance service offerings and improve efficiencies. All technology infrastructure, including cloud-based processing and storage, has undergone rigorous governance and risk assessment processes to, among other requirements, ensure adherence to all regulatory requirements, and has been deemed suitable for use. All our technology infrastructure adheres to our information security requirements.

Do you transfer personal information outside of South Africa?

Personal information will generally be processed in South Africa. In certain circumstances, unless contractually agreed otherwise, Sanlam may transfer personal information to countries outside of South Africa provided that the recipient is subject to a law, binding corporate rules or binding agreement which effectively upholds the principles for lawful processing of personal information as contained in POPIA, and such law, binding corporate rules or binding agreement contains similar restrictions to further cross-border transfers as those contained in POPIA.

If an intended foreign recipient of personal information is not subject to any such law, binding corporate rules or binding agreement, Sanlam will obtain the consent of the data subject prior to transferring the personal information to the third party. Where Sanlam transfers personal information to third parties outside of South Africa, it will do so only in accordance with, and in the fulfilment of its contract with the responsible party unless otherwise required or permitted by law.

How will you ensure that the quality of the personal information you hold is good enough for the purposes for which it was collected, that it is complete, accurate, not misleading, and updated where necessary?

The quality of information is both a factor of the input from the provider of the information and the steps taken in the actual processing of the information. Whilst Sanlam makes every reasonable effort to ensure that the personal information processed is complete, accurate and not misleading, it relies on other role players to do the same when submitting personal information to Sanlam. Sanlam also performs limited system validation checks to ensure the accuracy of personal information.

Has Sanlam identified any instances in which Sanlam must obtain prior authorisation from the Information Regulator to process personal information?

No.

Does Sanlam map or document the activities it performs for clients, and does the mapping or documentation include information about the requirements in terms of POPIA?

Yes, to both questions. All processes were revisited end-to-end bearing POPIA requirements in mind.

Have you performed a privacy impact assessment?

Yes, this is part of our POPIA processes.

Have you amended your compliance programme to manage privacy risks?

Yes, confidentiality of data has always been a priority and formed part of compliance programmes to manage privacy risks. These programmes have been enhanced to take POPIA requirements into account.

Does Sanlam outsource any of its activities? If so, to whom has Sanlam outsourced and what security measures has Sanlam put in place to ensure personal information is treated confidentially?

Yes, Sanlam may outsource some functions (for example, printing of benefit statements). Before outsourcing, risk assessments are conducted to ensure that the vendors have appropriate controls in place to safeguard personal information. Sanlam also ensures that its contracts with these vendors require them to secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and the unlawful access to or processing of personal information.

Do you provide personal information to anyone other than the bearers, legally appointed service providers or statutory authority of a client?

In addition to the service providers that form part of the contracted value chain, personal information is only provided to the client's appointed service providers to fulfil their contractual obligations, where written evidence of such appointment is provided to Sanlam. Similarly, personal information is provided to office bearers of a client, in accordance with legislation and/or to statutory authorities.

In the case of retirement funds or schemes, are there any activities Sanlam performs (where personal information is processed) that are not provided for in the agreement(s) with the retirement fund or scheme?

No.

What security measures are in place in relation to processes where bank account numbers are collected on hardcopy forms?

In the limited cases where we receive a hardcopy form, the document is scanned and indexed, and the original is either filed securely or shredded (depending on the type of document and contract with the client).

How and when will reporting on breaches be provided?

Sanlam's Information Security department have dedicated teams who monitor activities on our network and devices on a continuous basis. This includes the monitoring and response to potential cyber threats and internal activities that may be suspicious.

Sanlam is currently enhancing its existing data breach process to ensure compliance with the provisions in POPIA. Our updated reporting process will be communicated during June 2021.

Do you have policies, manual and other formal documentations in relation to POPIA and PAIA?

Yes. Below is the status of some of our documents which will be provided in due course:

Document	Status
Data Breach Process	Existing process is being enhanced for POPIA requirements.
Data Subject Participation Process	Process is being finalised.
Clean Desk Policy	In place
Privacy Statement	Document is being finalised
Retention and Destruction guidelines	Existing process is being enhanced for POPIA requirements.

Do you employ appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information?

Yes, Sanlam has a formal Information Security Strategy, inclusive of cybercrime prevention measures. The strategy is driven and governed by the Sanlam Group Office. The execution of the controls and preventative processes are coordinated and executed by Sanlam's Group Technology and Information division. Governance is managed via a number of governance forums (representing all the businesses in the Sanlam Group) that reports quarterly to the Group Office and the Sanlam Board. The strong focus on governance ensures that the business culture is aligned with the structures put in place to secure the information we manage.

The Information Security Statement (which can be provided on request) provides further details around our Information Security strategy and actions.

Have your employees been trained on POPIA and its requirements?

Yes, Sanlam has leveraged its internal training capabilities to provide both training and regular awareness and updates to employees. This was supplemented with additional external training sessions for key employees to ensure the principles of POPIA are entrenched in all levels in the organisation. These initiatives are ongoing, with regular training and awareness planned going forward. POPIA is not just about complying to legislation. It is also about a company's privacy culture.

What are some practical measures that Sanlam has put in place or is putting in place to ensure POPIA compliance?

Sanlam has implemented or is in the process of implementing various measures to ensure we comply with POPIA, including:

- Appointing an Information Officer.
- Reviewing all our contracts to ensure compliance with POPIA.
- Reviewing all our forms, communications and digital channels to ensure we are aligned with requirements in terms of POPIA.
- Enhancing privacy notices to inform data subjects how and why their personal information is/will be processed.
- Enhancing our existing system processes and data security controls to ensure compliance, within a rapidly changing technology environment.
- Ensuring the legal justification for the processing of personal information is clearly established.
- Enhancing existing processes for data subjects to access and review their personal information held by Sanlam.
- Enhancing our existing data breach processes.
- Increasing awareness and training among our staff about the regulatory requirements and enhancing our data privacy culture.
- Ensuring personal information continues to be stored and destroyed in a secure and confidential manner.

How will these changes impact on Sanlam's clients (members, brokers, intermediaries, employers, funds)?

Some of the above actions may require further engagement with our clients and service providers or changes to established processes, forms and digital channels.

Sanlam will ensure that any changes made will follow the proper governance processes and will be aligned with our usual client-focussed approach. Where changes directly impact or change how we engage, we will communicate this change and the reason for the change with the impacted parties.

