


		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 1 of 9

## TABLE OF CONTENT

- 1 Purpose
- 2 Scope
- 3 Definitions
- 4 Obligations and consequences
- 5 Forms of stored information
- 6 Timeline
- 7 General guidelines
- 8 Conditions of lawful processing
- 9 Steps to comply.
- 10 Review and approvals
- 11 References


### 1. PURPOSE

#### The purpose of the Act is to:

- Give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at –
  - Balancing the right to privacy against other rights, particularly the right of access to information; and
  - Protecting important interests, including the free flow of information within the Republic and across international borders.
- Regulate the way personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.
- Provide persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act; and
- Establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for, and to promote, enforce and fulfil the rights protected by the Act.

The purpose of this document is to ensure CANSA complies to this act.

The policy provides guidelines how the Policy is to be implemented.


		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 2 of 9

## 2. SCOPE

The act is applicable to all members of the CANSA Board of Directors, CANSA personnel, contracted personnel, CANSA volunteers, contracted volunteers, members, and service providers.

## 3. DEFINITIONS

POPI act:	Protection of Personal Information Act, 2013 (Act No 4 of 2013). POPIA: The Protection of Personal Information Act – the law that provides protection of personal information.
PAIA:	Promotion of Access to Information Act, 2000 (Act No 2 of 200) - the law that gives the right to access personal information.
Information Regulator (IR):	Juristic body established in terms of POPIA to see that there is compliance with both the act and Promotion of Access to Information Act (PAIA)
CANSA:	Cancer Association of South Africa.
Data subject:	The person to whom the information relates. For example: stakeholders, sponsors, donors, patients, clients, partners, suppliers, personnel, volunteers.
Special data subjects:	Children under 18 and patients.
Personal information:	Any information in any form – electronic and paper-based files – including information but not limited to identity number, name, surname, sex, pregnancy, marital status, nationality, colour, sexual orientation, age, physical or mental health, well-being, disability, conscience, belief, culture, language, criminal, and employment history.
Special personal information:	Information specific to information categories such as religion, race, ethnical origin, membership of a

		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				FIN-PL-ADM-005
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 3 of 9

trade union, political affiliation, sexual life, medical information, biometrical information (blood type, fingerprints)

Processing:

Any activity (automated or manual) such as collection, receipt, recording, organising, storage, collation, retrieval, alteration, updating, distribution, dissemination by transmitting, erasure or destructing.

Responsible party:

the person who determines why and how to process. For example: companies, non-profit companies, governments, state agencies and people.

Operator:

the person who processes personal information on behalf of the responsible party. For example: if CANSA were to outsource payroll.

EXCO:

Executive Committee of CANSA

Data bridge:


Unlawful, unauthorised disclosure of personal data – either accidental or deliberate.

Information officer:

Person in CANSA registered with the regulator responsible to ensure that the POPI act is implemented.

Deputy Information officer:

The deputised information officer. The CEO has designated Head: Admin, IT, Procurement as information officer: Person supporting the Information officer whom the Information officer delegates to.

		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 4 of 9

#### 4. OBLIGATIONS AND CONSEQUENCES

All organisations, companies and institutions in South Africa must comply with POPIA. CANSA as a registered Non-profit company will have to comply with POPIA. Various obligations are placed on the responsible party, which is the body ultimately responsible for the lawful processing of personal information:

- To regulate the collection and processing of personal information in a manner that will safeguard such information against unauthorised access and usage.
- To establish the requirements and conditions for the collection, distribution, and retention of personal information in line with the act.
- To determine the purposes for which personal information will be used.
- To ensure only operators (e.g., Security, contracted telemarketers etc. and third parties (e.g., suppliers) that can meet the requirements of lawful personal information processing prescribed by POPIA are used.
- Personal information should only be processed if it is adequate, relevant, and not excessive i.e., only collect information which is needed.

CANSA EXCO supported by the information officer and deputy information officer of CANSA are responsible for administering and overseeing the implementation of this policy and any applicable supporting guidelines and procedures.


Violations of this policy and of the POPI act will be dealt with by the Information Regulator. Data subjects may refer their complaints to the Information Regulator.

There are two legal consequences for the responsible party in case of a data breach:

- A fine or imprisonment of between R1 million and R10 million or one to ten years in jail
- Financial compensation to data subjects for the damage they have suffered.

Other consequences:

- Reputational damage
- Losing customers

		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 5 of 9

- Losing employees
- Failing to attract new stakeholders, sponsors, donors, volunteers and so forth.
- Security compromise could occur with back door access to the financial institutions' information in that cybercrime could occur.

## 5. FORMS OF STORED INFORMATION

Data is stored in the following ways:


- Electronic database
- Manual filing system
- Address books, calendars, diaries
- Payroll system
- Sent and received via e-mail stored via cloud.
- Contracts
- Sign in registers at reception
- Telephone records
- Invoices, orders, quotes
- Application forms
- Attendance registers
- Meeting recordings – zoom, Skype, Microsoft Teams,

## 6. TIMELINE

The deadline for organisations to comply is 1 July 2021.

## 7. GENERAL POLICY GUIDELINES

- It is each organisation, company, institution's obligation to do what is reasonably expected to ensure that data is protected, and information is kept safe.
- Data should rather be stored in a cloud and not on computers or external hard drives.

		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 6 of 9


- Computers should not be left unattended, and screens should be locked.
- Responsible parties must ensure that information quality is complete, accurate, not misleading and updated. Assurance should also be in consent forms and terms and conditions.
- PAIA promotes access to information in terms of section 32(1)(a) of the constitution. Therefore, both PAIA and POPIA must be implemented. A manual must be developed, monitored, maintained, and made available.

## 8. CONDITIONS FOR LAWFUL PROCESSING


- Accountability – responsibility to ensure compliance.
- Processing limitations – only process information, which is adequate, relevant and not excessive.
- Purpose specific – explicitly defined.
- Further processing limitations – only process data if it forms part of the originally obtained purpose.
- Information quality – Ensure that information is complete, accurate, not misleading and updated.
- Openness – notify data subjects about the circumstances in which such compliance would be mandatory e.g., where the law authorises the processing.
- Security safeguards – this is the list of measures that should be taken to prevent loss, damage, unauthorised and unlawful access.
- Data subject participation – they have the right to request the records kept on them and how their information was shared.

## 9. STEPS TO COMPLY

- Data subjects be informed of the purpose or reason for the collection of their data, so that they may give consent or refuse it.
- Any further use of the collected personal information - must be compatible with the initial purpose of collection. All information that is collected by CANSA may only be used for the initial purpose for which it was collected.

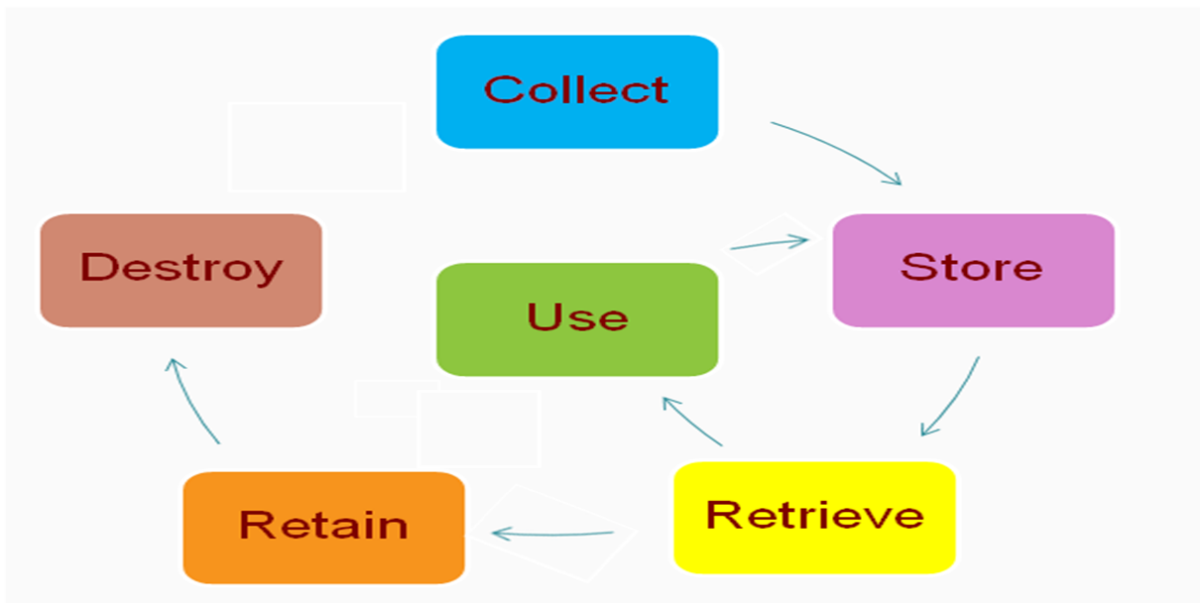
		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
			<b>Version no.</b>	01	<b>Page</b>	FIN-PL-ADM-005
		<b>Date prepared</b>				Page 7 of 9

- CANSA - may not process a data subjects' information without consent unless imposed by law, in public interest, or to complete a project which the data-subject is party to.
- Consent is given by a data-subject by signing an agreement or application or a tick box on a form. This could read: "I \_\_\_\_\_ herewith give permission that personal information which is required for the project/service/event/programme may be stored on a paper-based and/or digital systems of CANSA and may be used for the purpose of the project/service/event/programme".
- Data subjects - must be advised of the consequence of not giving consent e.g., not participating in an activity.
- If CANSA seeks to use the information for another purpose, the data subject - must be contacted to obtain consent for further processing.
- The data subject may revoke his/her consent at any time. The withdrawal of consent must be communicated to the Information Officer in writing within a reasonable time. The withdrawal will be subject to any contract that is in place. The withdrawal will only be effective if CANSA agrees in writing. The data-subject will be informed of the consequences of the withdrawal as it will result in CANSA being unable to provide services or benefits.
- CANSA will not keep personal information of data-subject for a specific purpose for longer than is necessary to fulfil the purpose of its collection unless further retention is required by law or the data subject's consent is obtained to make provision for further retention.
- Once the purpose of retention of the information is fulfilled the information will be destroyed in accordance with the POPI Act.
- CANSA will take all reasonable steps are taken to ensure secure data transmission over the internet or via its online services.
- Data is only collected with consent from the data subject. CANSA relies on data subjects for correctness of information. The Data subjects are required to confirm the correctness of information.


		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 8 of 9

- An Information Officer of CANSA must be registered with the Information Regulator.
- A client/patient information confidentiality policy is dealt with under the Patient Confidentiality Policy, which also complies with the provisions of the POPIA.
- Existing policies must be reviewed to comply with the POPIA and be reviewed every two years.
- Employees must be made aware of POPI and CANSA's policy.
- Employment contracts with personnel who work with information of data subjects must comply with the Act.
- Data breaches must be reported to the Information Regulator and data subjects.
- A data breach response plan must be developed.
- A PAIA manual must be developed and published on the CANSA website and lodged with the Information Regulator.

The cycle of how information is dealt with can be illustrated as follows:





		<b>POLICY and GUIDELINE</b>			<b>Doc. No.</b>	
		<b>Protection of Personal information (POPI) Act</b>				
	<b>Date prepared</b>		<b>Version no.</b>	01	<b>Page</b>	Page 9 of 9
						FIN-PL-ADM-005

All references/resources utilised in compiling this guideline document.

<https://www.golegal.co.za/popia-compliance-data-breach/>

<https://popia.co.za/>

<https://www.elsabeklinckassociates.co.za>