

**DOCUMENT: SABS PRIVACY POLICY****DEPARTMENT: LEGAL, RISK & COMPLIANCE****Compiler:** J. Leotlela:**Signature:** **Approving Officer:** J. Scholtz**Signature:** **To be revised by:**

2025-11-30

**Page 1 of 13****Document No.**

CPP 281

**Revision No.**

Ø

**Effective date:**

2022-12-01

**Contents**

SECTION A: CORPORATE POLICY .....	2
1. Policy statement.....	2
2. Objectives .....	2
3. Scope.....	2
4. Definitions/Abbreviations .....	3
5. References.....	4
6. Legislative, standards and codes requirements .....	5
7. Rules and Principles .....	5
SECTION B: STANDARD OPERATING PROCEDURE .....	5
8. Procedure .....	5
8.1. Process.....	6
8.2. Roles and Responsibilities .....	12
8.3. Monitoring and reporting.....	12
SECTION C: ADMINISTRATION AND CONTROL .....	13
9. Replacement and withdrawal.....	13
10. Revision/Amendment particulars .....	13

**CONTROLLED DISCLOSURE**

When downloaded from the SABS Document Management System, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

**SECTION A: CORPORATE POLICY****1. Policy statement**

The Constitution of the Republic of South Africa, 1996 recognises and protects the right to privacy as one of the basic human rights. To ensure the protection of this right, the Protection of Personal Information Act, No. 4 of 2013 (POPIA or the Act) was promulgated and became law from 1 July 2020. This law applies to both public and private entities, which, in one way or the other process Personal Information.

Compliance with POPIA is mandatory to any person who, or any organisation which, keeps any type of records relating to Personal Information of anyone or any entity, unless those records are subject to other legislation which protects such information more stringently. Therefore, POPIA provides the minimum requirements to comply with for the collection, safe keeping and generally, processing of Personal Information.

**2. Objectives**


The objectives of this CP are to:

- 2.2 establish a compliance framework within SABS and SABS Commercial SOC Ltd regarding the processing of personal information
- 2.2 to recognise and comply with any limitations applicable when processing personal information in possession of SABS and/ or SABS Commercial.

**3. Scope**

This policy applies to any person or entity processing Personal Information for or on behalf of SABS and SABS Commercial SOC Ltd, such as:

- a) employees
- b) contractors
- c) agents
- d) service providers
- e) consultants, etc.

<p><b>DOCUMENT: SABS PRIVACY POLICY</b></p> <p><b>DEPARTMENT: LEGAL, RISK &amp; COMPLIANCE</b></p>		To be revised by:
		2025-11-30
		Page 3 of 13
		Document No.
		CPP 281
		Revision No.
		Ø

In this policy, any reference to SABS shall be deemed to include SABS Commercial SOC Limited and vice versa.

#### 4. Definitions/Abbreviations

The following definitions are, where applicable, imported from the POPIA and are being used herein to foster consistency in terminology between this policy and the POPIA:

- 4.1 **“Data Subject”** means either individuals or juristic persons to whom personal information relates such as, recruits, employees, suppliers, customers, etc.
- 4.2 **“Deputy Information Officer”** or **“DIO”** means an employee of the SABS or SABS SOC Commercial Ltd who has been duly appointed as such with specific roles to assist the Information Officer in executing his/ her responsibilities as required by POPIA and PAIA;
- 4.3 **“Information Officer”** means the Chief Executive Officer of the SABS and SABS Commercial SOC Ltd or anyone acting in such position or capacity;
- 4.4 **“Operator”** means a person who processes Personal Information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party, such as suppliers, contractors, etc.
- 4.5 **“PAIA”** means Promotion of Access to Information Act, Act 2 of 2000;
- 4.6 **“Personal information”** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:
  - (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
  - (b) information relating to the education or the medical, financial, criminal or employment history of the person;
  - (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person, etc.



- 4.7 **“POPIA” or (the Act)”** shall mean Protection of Personal Information Act, No. 4 of 2013;
- 4.8 **“Processing”** means any operation or activity or any set of operations, whether by automatic means, concerning Personal Information, including:  
the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.  
dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure, or destruction of information.
- 4.9 **“Responsible Party”** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing Personal Information.
- 4.10 **“SABS”** means the South African Bureau of Standards; and
- 4.11 **“SABS Commercial”** means SABS Commercial SOC Ltd, being a company wholly owned by the SABS.

## 5. References

This document should be read in conjunction with:

CSP 101 – Legal Services of the SABS

CP211 - IT Security and Access Control Policy

CP 211 – ICT Security and Access Control Standard Operating Procedure

CSP 124 - Record Management

CSP 601 - Recruitment and Selection Procedure and Relocation

CPO 610A - Remuneration

CPO 611B – Performance Management

CPO 614 – Recruitment and Selection

CPO 615 – Employee well-being Programme.

## 6. Legislative, standards and codes requirements

The following legislation inform and were considered when developing this policy:

- a) The Constitution of the Republic of South Africa, 1996
- b) Protection of Personal Information Act, (No. 4 of 2013)
- c) Promotion of Access to Information Act, (No. 2 of 2000)
- d) Promotion of Administrative Justice Act, (No. 3 of 2000)
- e) Standards Act, (No. 8 of 2008)
- f) Public Finance Management Act, (No. 1 of 1999)
- g) King IV Code on Corporate Governance

## 7. Rules and Principles

As an entity in possession of Data Subjects' Personal Information, the SABS is required to comply with POPIA. SABS has a legal obligation to ensure the safety, confidentiality, and lawful processing of Personal Information in its custody or under its control. To assist SABS in carrying out this legal obligation, and as is required in terms of POPIA, the SABS has appointed an **Information Officer** ("IO") and **Deputy Information Officers** (DIO) from each Business Unit. SABS acknowledges that it is a **Responsible Party** where it uses the services of third parties, and it is also an **Operator** when it is being employed as a service provider.

## SECTION B: STANDARD OPERATING PROCEDURE

### 8. Procedure

To ensure compliance with POPIA the following procedure must be followed when processing personal information:

- a) Obtain consent to process Personal Information.
- b) Only the minimum amount of Personal Information necessary to allow a decision to be taken should be obtained / requested;
- c) All Personal Information must be treated as confidential and must be safely kept;

- d) Any unlawful or unauthorised access to the Personal Information under the control of SABS must immediately be reported to the appointed DIO in the affected BU/ Department who must as soon as possible report same to the IO;
- e) Personal Information of Data Subjects may only be retained for the amount of time as permitted by the law or by way of contractual agreement;
- f) Destruction or deletion of Personal Information under the control of SABS must be done with the permission of the IO; and
- g) A list of appointed DIO shall be published and updated as and when necessary.

### 8.1. Process

The following explains the process for the implementation of 8 conditions laid down in Section 8 of POPIA for lawful processing of Personal Information and the measures to be implemented to give effect to these conditions:

- a) **Accountability** – SABS is accountable for the *Personal Information* it *Processes* or allows to be *Processed* on its behalf. SABS is therefore committed to ensure that the *Personal Information* of all *Data Subjects* in its possession or under its control is collected, stored, used, applied, shared and/ or destroyed appropriately, securely and without comprising the privacy rights of *Data Subjects*.
- b) **Processing limitation** – SABS as an organ of state, an employer and through its commercial activities shares information (Data Subjects' Personal Information) with external entities (the Operators). SABS also collects Personal Information. Accordingly, SABS is also a primary source of personal information. For this reason, the SABS shall ensure that personal information is processed lawfully, reasonably and in a manner that does not infringe the rights of the data subject. The SABS shall ensure that it collects Personal Information, which is adequate, relevant and not excessive, given the purpose in respect of which the Personal Information is processed.



ALL SABS' employees, contractors, consultants, etc., must when Processing Information:

- (i) Uphold, as far as is reasonably possible, the principle of minimality – where only adequate, relevant, and necessary data and/or information is processed to achieve the purpose for which the information was obtained.
  - (ii) Develop and communicate processes and enhance the developed processes, where feasible, to enable Data Subjects to: Object, where reasonable and lawful, to the processing of their Personal Information, request that their Personal Information be updated or corrected, and request and facilitate, where legally feasible, the deletion of Personal Information or restrict processing and access to the Personal Information. The SABS is committed to collect and process Personal Information in a reasonable way that does not infringe on the privacy rights of the Data Subjects. While in terms of the Act the Data Subject has the right to withdraw his/her/its consent, it is advisable that legal advice be sought in instances where there might be a need to still process the information despite the withdrawal.
- c) **Purpose Specification** – Only *Personal information* that relates to a specific, explicitly defined and lawful purpose related to a function or activity of the SABS may be collected. It is the responsibility of every department within SABS to develop a checklist of *Personal Information* that is required in their execution of duties. This is necessary to ensure that only relevant, explicit and fit for purpose Personal Information is obtained for each departmental needs.
- (i) Any medium used within or from SABS to collect *Personal Information* from *Data Subjects*, e.g contracts, forms or websites must contain a consent by

<p><b>DOCUMENT: SABS PRIVACY POLICY</b></p> <p><b>DEPARTMENT: LEGAL, RISK &amp; COMPLIANCE</b></p>	<p><b>SABS</b></p>	To be revised by:
		2025-11-30
		Page 8 of 13
		Document No.
		CPP 281
		Revision No.
		Ø

the *Data Subject* for collection and processing of *Personal Information*, except where the Act prescribes otherwise.

- d) **Retention and restriction of records:** Personal Information shall not be retained any longer than is necessary to achieve the purpose for which the information was collected and processed or as otherwise permitted in law, or by way of contractual agreement. All *Personal Information* in possession of SABS or under its control must be retained for a maximum period prescribed by law, e.g. five years from expiry or termination of the transaction, or as prescribed in terms of the contract or as per operational requirements.
- (i) Personal Information under the control of the SABS shall be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form.
  - (ii) It is recognised that documents and records can either be in electronic or hard copies format. Each Department or Business Unit of SABS shall, with guidance from Legal Department, classify its records and keep a **classification list of records** and reasonable security safeguards shall be employed in the storage and retention of internal information.
  - (iii) Together with record classification, the Business Units shall define the life cycle of their documents and records within the SABS as part of the measures implemented to give effect to the conditions of processing Personal Information.
  - (iv) The following mechanism regarding documents and records retention and deletion shall be implemented by all Business Units within SABS:
    - records requested by Operators, must contain only the minimum amount of content necessary to allow a decision to be taken;
    - documents and records must always be safely secured and stored in such a way as to maintain confidentiality and the integrity of the content;




- documents may not be shared, communicated or transmitted, unless authorised, in writing by employees with delegated authority;
- only the “final” draft of documents will be stored and retained;
- documents will not be duplicated or retained indefinitely, unless authorised by the Information Officer; and
- issue directives, that do not conflict with the Act, but advances the purpose of the Act, on how to process Personal Information.

**e) Further processing**

It is the responsibility of every employee of SABS to ensure that any additional processing of Personal Information by itself is compatible with the original purpose for which Personal Information was collected. The adopted measures must apply to Operators.

**f) Information quality**

In obtaining Data Subjects' Personal Information, every SABS employee, consultant, etc., shall ensure that s/he or it obtains Personal Information that is up to-date, accurate, complete and not misleading.

<p><b>DOCUMENT: SABS PRIVACY POLICY</b></p> <p><b>DEPARTMENT: LEGAL, RISK &amp; COMPLIANCE</b></p>		To be revised by:
		2025-11-30
		Page 10 of 13
		Document No.
		CPP 281
		Revision No.
		Ø

**g) Openness**

In order to be able to respond to requests for information in terms of PAIA, the SABS has developed a PAIA Manual with detailed information regarding

- (i) the categories of record by the SABS which are available without a person having to request access in terms of PAIA;
- (ii) a description of the records of the SABS which are available in accordance with any other legislation;
- (iii) sufficient detail to facilitate a request for access to a record in possession or under the control of the SABS,
- (iv) a description of the subjects on which the SABS holds records and the categories of records held on each subject; and
- (v) such other information as may be prescribed therein.

**h) Security safeguards**

The ICT department of SABS shall ensure continuous implementation of reasonable technical and organisational measures, having regard to generally accepted information security practices and procedures which applies to it generally or as required in terms of specific industry rules or professional rules and regulations, to prevent loss of, damage to or unauthorised destruction of Personal Information and unlawful access to or processing of personal information. All SABS's employees, consultants, interns, etc., shall comply with CP 211 - IT Security and Access Control Policy and CP 211 – ICT Security and Access Control Standard Operating Procedure.

<p><b>DOCUMENT: SABS PRIVACY POLICY</b></p> <p><b>DEPARTMENT: LEGAL, RISK &amp; COMPLIANCE</b></p>	<p><b>SABS</b></p>	<p>To be revised by:</p>
		<p>2025-11-30</p>
		<p>Page 11 of 13</p>
		<p>Document No.</p>
		<p>CPP 281</p>
		<p>Revision No.</p>
		<p>Ø</p>

## 8.1.2 Notification of Security Compromises

**8.1.3** Any unlawful or unauthorised access to confidential information or Personal Information in the custody of the SABS must, as soon as practicable, be reported to the Legal Department which shall in turn report such to the Information Regulator and the Data Subjects affected in the prescribed manner.

Such notification must include the following:

- information about the compromise;
- a description of the possible consequences and dangers of the compromise;
- a description of the measures taken or to be taken to remedy the compromise;
- a recommendation regarding measures to be taken by the Data Subjects to mitigate the possible adverse effects of the compromise to themselves, and
- if known, the identity of the perpetrator.

**8.1.3.1** To comply, with its reporting requirements to the Information Regulator, its obligations to notify Data Subjects and to develop management mitigation strategies, the SABS Legal Department with the assistance of the ICT Department and/ or any other affected department in SABS will follow the process below should an information breach or compromise occur:

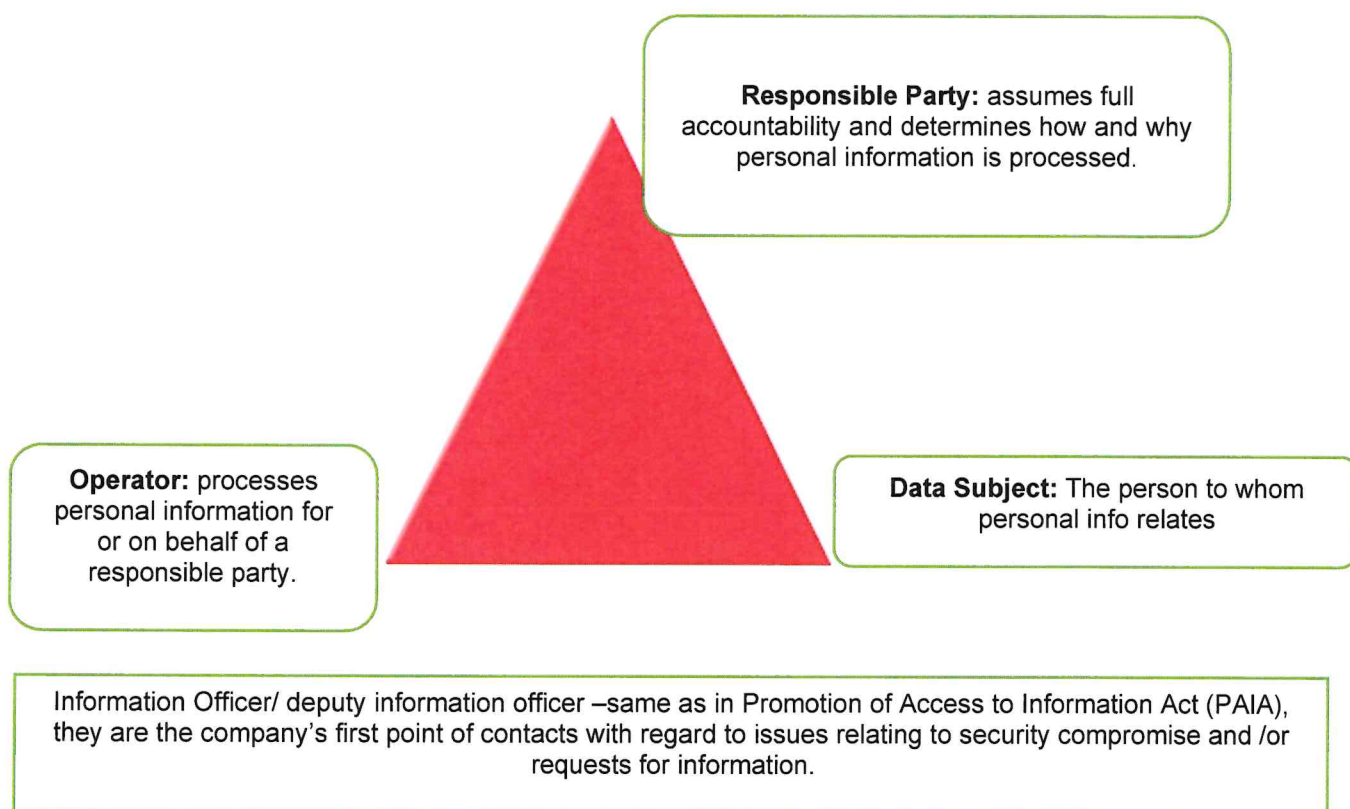




<p><b>DOCUMENT: SABS PRIVACY POLICY</b></p> <p><b>DEPARTMENT: LEGAL, RISK &amp; COMPLIANCE</b></p>	<b>SABS</b>	To be revised by:
		2025-11-30
		Page 12 of 13
		Document No.
		CPP 281
		Revision No.
		Ø

## 8.2. Roles and Responsibilities

### PARTIES IN POPIA



## 8.3. Monitoring and reporting

- The implementation of the procedure will be monitored through the assistance of the appointed DIO.
- Any unlawful or unauthorised access (breach) to Personal Information under the control of SABS shall be reported to the Information Regulator by the Information Officer.

**SECTION C: ADMINISTRATION AND CONTROL****9. Replacement and withdrawal**

This document is new, and it does not replace any SABS policy

**10. Revision/Amendment particulars**

<b>Rev. No.</b>	<b>Effective date</b>	<b>Nature of Revision</b>
Ø	2022-12-01	New Document