correctional services

Department:
Correctional Services
REPUBLIC OF SOUTH AFRICA

DCS

PROTECTION OF PERSONAL INFORMATION

(POPIA)

POLICY

Table of Contents **Page**

1. EXECUTIVE SUMMARY

1.1. The Protection of Personal Information Act, No. 4 of 2013 (POPIA) establishes rules and practices that organisations must follow when processing personal information of both natural and juristic persons.

1.2. This policy provides guidance to employees of the Department of Correctional Services (DCS) on the lawful implementation of POPIA, thereby advancing the constitutional right to privacy while balancing the right of access to information and the Department's primary mandate of security, safety, and good order.

1.3. The DCS will operationalise the eight guiding principles of POPIA, granting rights to data subjects in respect of their personal information and imposing obligations on the Department and its employees to ensure compliance and safeguard data.

2. SCOPE AND APPLICATION

2.1. This policy applies to the processing of all personal information by the Department of Correctional Services (DCS), and is binding on all employees, contractors, and operators acting on its behalf.

2.2 The policy governs the personal information of all data subjects interacting with the DCS, including but not limited to:

* Employees and officials.
* Inmates, parolees, and probationers.
* Awaiting trial persons.
* Visitors, contractors, and service providers.
* Victims, complainants, and whistle-blowers.
* Legal representatives and other stakeholders.

2.3. The Department acknowledges that the nature and extent of protection afforded to personal information is contextual. The application of this policy will be balanced against other legislative mandates, primarily the Correctional Services Act (Act 111 of 1998), and the fundamental requirements of security, safety, and good order within correctional facilities.

2.4. Recognising the unique status of persons within the criminal justice system, this policy provides a framework for the lawful limitation of certain data subject rights where such limitation is justified, necessary, and proportionate in a democratic society, as contemplated in Section 36 of the Constitution and specific exemptions within POPIA.

3. DEFINITIONS AND ABBREVIATIONS

- **Biometrics:** Personal identification techniques based on physical, physiological, or behavioural characteristics (e.g., blood typing, fingerprinting, DNA analysis, retinal scanning, voice recognition).
- **CCTV**: Closed Circuit Television.
- **Child**: A natural person under 18 years who is not legally competent, without the assistance of a competent person, to act or decide on personal matters.
- **Consent**: Voluntary, specific, and informed expression of will permitting the processing of personal information.
- **Competent Person**: A legally authorised person who may consent on behalf of a child. For children in the care of or interacting with the DCS, this includes a parent, legal guardian, or a designated social worker .
- **Data Subject:** The natural or juristic person to whom personal information relates.
- **De-Identify**: To delete or modify information that identifies a data subject, or can reasonably be used to identify one.
- **DCS**: Department of Correctional Services.
- **Electronic Communication**: Text, voice, sound, or image messages transmitted and stored over electronic networks.
- **High-Sensitivity Information:** Personal information which, if disclosed, could cause significant harm to the data subject or compromise the security of a DCS facility. This includes, but is not limited to: Identity Numbers, financial data,

medical/psychological records, biometric data, information on security operations or gang affiliations, and personal information of victims and whistle-blowers.

- **Information Officer**: The Accounting Officer responsible for ensuring compliance with POPIA.
- **Operator:** A person or entity processing personal information for a responsible party, under a contract or mandate, without direct authority from that party.
- **PAIA**: Promotion of Access to Information Act, No. 2 of 2000.
- **Personal Information:** Any information that can identify a person, including demographic, biometric, health, financial, or cultural details.
- **POPIA**: Protection of Personal Information Act, No. 4 of 2013.
- **Privacy Notice:** A document that explains how personal information is collected, used, and safeguarded by DCS.
- **Processing**: Any operation (manual or automated) performed on personal information, including collection, storage, use, dissemination, modification, or destruction.
- **Publicly Available Information**: For the purposes of this policy, information is not considered "publicly available" merely because it was reported in the media or disclosed in court proceedings. The DCS remains obligated to protect the accuracy, security, and responsible use of any personal information in its custody.
- **Responsible Party**: The entity that determines the purpose and means of processing personal information—in this case, the DCS.
- **Re-Identify**: To re-establish the identity of a data subject from de-identified information.
- **Unique Identifier**: A distinctive reference assigned to a data subject by the responsible party for operational purposes.
- **Special Personal Information:** Information relating to religious or philosophical beliefs, race, ethnic origin, trade union membership, political persuasion, health, sex life, or biometric data.

4. BACKGROUND

4.1. The right to privacy is entrenched in section 14 of the Constitution of the Republic of South Africa, 1996. POPIA gives effect to this right by regulating the lawful processing of personal information.

4.2. The DCS recognises the importance of safeguarding privacy and is committed to collecting, processing, storing, and destroying personal information responsibly and confidentially, while preventing unauthorised access.

5. POLICY MANDATE

This policy is mandated by POPIA and supported by related legislation, including but not limited to:

- Promotion of Access to Information Act, 2000 (PAIA).
- National Archives and Records Service of South Africa Act, 1996.
- Promotion of Administrative Justice Act, 2000.
- Public Finance Management Act, 1999.
- Companies Act, 2008.
- Electronic Communications and Transactions Act, 2002.
- National Credit Act, 2005.
- Consumer Protection Act, 2008.
- Correctional Services Act, 1998 (Act No. 111 of 1998).
- Protection from Harassment Act, 2011.
- Cybercrimes Act, 2020.
- Electronic Deeds Registration Act, 2019.
- Financial Intelligence Centre Act, 2001.

- Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.
- Relevant data protection regulations and other applicable legislation.
- South African Protected Disclosures Act, 2000

6. POLICY STATEMENT

The DCS is committed to protecting personal information in its custody and to ensuring lawful, transparent, and consistent processing in line with POPIA, the Correctional Services Act, and related laws. All employees and stakeholders must comply with this policy when processing personal information on behalf of the Department.

7. POLICY OBJECTIVES

The objectives of this policy are to:

- Ensure DCS complies with the obligations imposed by POPIA.
- Promote the protection of personal information in line with applicable regulatory standards.

8. POLICY PRINCIPLES AND EMPLOYEE OBLIGATIONS

All employees and stakeholders processing personal information on behalf of the DCS are personally responsible for adhering to the following enumerated principles:

8.1 **Accountability:**

8.1.1. Departmental Obligation: The DCS, as the responsible party, remains accountable for complying with the conditions for lawful processing.

8.1.2. Employee Obligation: You are personally accountable for the personal information you access and process. You must complete mandatory POPIA training and adhere strictly to the procedures in this policy.

8.2. **Processing limitations**:

8.2.1. Employee Obligation: You may only process personal information where you have a clear and lawful reason to do so, linked directly to your official duties under the Correctional Services Act or other law. You may not process information for personal gain, curiosity, or outside of your mandate.

8.3. **Purpose Specification:**

8.3.1. Employee Obligation: When collecting information, you must be able to identify and justify the specific, lawful purpose for which it is being collected.

8.4. **Further Processing Limitation:**

8.4.1. Employee Obligation: You may not use personal information collected for a completely different, unrelated purpose (e.g., research) to your primary duty or lawful instruction without a lawful basis and prior authorisation from the Information Officer or delegated authority.

8.5. **Information quality:**

8.5.1 Employee Obligation: You must take reasonable steps, to ensure that the personal information you use and record is accurate, complete, not misleading, and updated where necessary.

8.6. **Transparency/Openness:**

8.6.1. Employee Obligation: You must, where practicable, inform data subjects that their information is being collected and the purpose for doing so. When responding to inquiries (e.g., from family members), you must follow strict verification protocols and may only disclose information as per DCS-approved procedures.

8.7. **Security Safeguards:**

8.7.1. Employee Obligation: You are required to protect the confidentiality and integrity of personal information. This includes using secure passwords, locking away physical files, not leaving sensitive information on desks or screens unattended, and immediately reporting any suspected loss, theft, or unauthorised access (a data breach) to your supervisor and the Information Officer.

8.8. **Data Subject Participation:**

8.8.1. Employee Obligation: You must respect the rights of data subjects to access and request correction of their personal information, as facilitated through the DCS's PAIA Manual.

8.8.2. Limitation of Rights: You must be aware that the DCS may lawfully limit these rights in accordance with POPIA where access would jeopardise the maintenance of law, order, and security, impair the privacy of another data subject, or where the request is manifestly unfounded or excessive.

9. FINANCIAL IMPLICATIONS

Costs will be incurred for staff training, awareness campaigns, system upgrades, and monitoring of compliance. Expenditure will be managed in accordance with the Public Finance Management Act (PFMA) and Treasury Regulations.

10. LEGAL IMPLICATIONS

10.1. This policy is binding on all DCS employees. Non-compliance will constitute misconduct and may result in disciplinary action in line with DCS policies and applicable labour law.

10.2. Employees must note that contravention of POPIA can, in certain circumstances, lead to criminal prosecution and personal liability for fines or imprisonment.

11. POLICY IMPLEMENTATION

11.1. Implementation will occur nationally across all DCS Branches and Regions. The Information Officer (the National Commissioner), supported by Deputy Information Officers, is responsible for ensuring overall compliance.

11.2. All heads of Branches and Regions are responsible for the implementation and monitoring of this policy within their respective areas of responsibility.

11.3. Data Breach Response:

11.3.1. All employees are obligated to understand and adhere to the Department's Data Breach Standard Operating Procedure (SOP).

11.3.2. This SOP provides the detailed steps for identifying, containing, assessing, reporting, and mitigating a data breach, in compliance with the mandatory notification requirements to the Information Regulator.

11.3.3. Any suspected or confirmed loss, unlawful access, or compromise of personal information must be reported immediately in accordance with the Data Breach SOP. Failure to report is a serious disciplinary offence.

12. POLICY REVIEW

This policy will be reviewed every five (05) years, or earlier if necessitated by legislative or operational changes.

APPROVED

MR T.A. THOKOLO
NATIONAL COMMISSIONER (ACTING)
DATE: 3/11/25