PAIA MANUAL FOR THE OFFICE OF THE MILITARY OMBUD

Prepared in terms of section 14 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)

English Final, No. 2

Date of Compilation: March 2026

Table Of Contents

Tables

Figures

FOREWORD

Access to information is a cornerstone of democracy and is enshrined as a fundamental human right in Section 32 of the Constitution of the Republic of South Africa, 1996. This right empowers individuals to make informed decisions and hold public institutions accountable.

The Office of the South African Military Ombud is committed to promoting transparency, accountability, and effective governance. In compliance with the Constitution and the Promotion of Access to Information Act, 2 of 2000 (PAIA), as amended, this Manual is published to guide the public on how to access records held by the Office, and to give effect to the constitutional right of access to information.

The implementation of PAIA will be balanced with other rights contained in the Bill of Rights, including the right to privacy as protected under the Protection of Personal Information Act, 4 of 2013 (POPIA).

As the Office processes personal information in the execution of its mandate, it remains committed to protecting such information and ensuring that it is handled lawfully, fairly, and transparently.

This Manual serves as a practical tool to facilitate access to information while respecting the principles of fairness, confidentiality, and the public interest.

LIEUTENANT GENERAL (RET) V.R. MASONDO
MILITARY OMBUD

DATE: 09/03/2026

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1. **DIO** – Deputy Information Officer

1.2. **DMO** – Deputy Military Ombud (Deputy Information Officer)

1.3. **DOD** – Department of Defence

1.4. **IO** – Information Officer

1.5. **MINISTER** – Minister of Defence and Military Veterans

1.6. **MO** – Military Ombud (Information Officer)

1.7. **OFFICE** – Office of the Military Ombud

1.8. **PAIA** – Promotion of Access to Information Act, 2 of 2000

1.9. **PFMA** – Public Finance Management Act, 1 of 1999

1.10. **POPIA** – Protection of Personal Information Act, 4 of 2013

1.11. **REGULATOR** – Information Regulator

1.12. **RELEVANT AUTHORITY** – Minister of Defence and Military Veterans

2. PURPOSE OF THE PAIA MANUAL

2.1. The purpose of this Manual is to:

2.1.1. Provide guidance on the process and mechanisms available for accessing records held by the Office in accordance with the Promotion of Access to Information Act, 2000 (PAIA);

2.1.2. Assist members of the public, employees, stakeholders, and other interested parties in understanding their rights and responsibilities under the PAIA and how to exercise them effectively.

2.2. This Manual specifically aims to:

2.2.1. **Facilitate Transparency and Accountability**: Ensure that information about the operations, policies, and decisions of the Office is accessible to the public, thereby fostering a culture of transparency and good governance.

2.2.2. **Describe the Categories of Information Held by The Office**: Provide details on the types of records maintained by the Office, including those that are automatically available and those that require a formal request.

2.2.3. **Explain the Process of Requesting Access to Information**: Outline the procedures, forms, and legal requirements involved in making a request for records under PAIA, ensuring that requesters understand their rights and obligations.

2.2.4. **Identify the Relevant Contact Details**: Provide information on the Information Officer and Deputy Information Officer who are responsible for handling PAIA requests and ensuring compliance with the Act.

2.2.5. **Clarify the Remedies Available for Denied Requests**: Inform requesters of the legal recourse available if their request for information is denied, including internal appeals and lodging complaints with the Regulator.

2.2.6. **Outline the Security and Privacy Measures for Personal Information**:[1] Describe how the Office processes and protects personal data in compliance with PAIA and the Protection of Personal Information Act, 2013 (POPIA).

2.2.7. **Assist the Public in Exercising Their Right of Access to Information**: Provide clear and concise guidance on how requesters can obtain information necessary for the exercise and protection of their rights.

3. ESTABLISHMENT OF THE OFFICE

3.1. The Office has been established in terms of the Military Ombud Act, 4 of 2012, as an independent and impartial statutory body. It serves as an oversight entity to handle complaints and ensure accountability within the

---

[1] Section 1 of the Protection of Personal Information Act, 4 of 2013 defines the term **'personal information'** to mean 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, wellbeing,
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, email
address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that
would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself
would reveal information about the person.

South African National Defence Force (SANDF) while upholding the principles of fairness, transparency, and the rule of law.

3.2. **Mandate and Responsibilities.** The Office is responsible for:

3.2.1. **Investigating complaints** lodged by:

3.2.1.1. Current members of the SANDF concerning their conditions of service.

3.2.1.2. Former members of the SANDF in relation to their conditions of service.

3.2.1.3. Members of the public regarding the official conduct of SANDF members.

3.2.1.4. Persons acting on behalf of a complainant, with appropriate authorization.

3.2.2. Ensuring fair and unbiased investigations into complaints to safeguard the rights and dignity of both complainants and SANDF members.

3.2.3. Making recommendations to the Minister of Defence and Military Veterans to improve issues related to military service conditions and personnel conduct.

3.2.4. Mediating and resolving disputes where appropriate, through conciliation and negotiation, without resorting to litigation.

3.2.5. Promoting compliance with constitutional principles in SANDF service conditions and conduct.

3.3. **Limitations and Exclusions**

3.3.1. While the Office provides an essential avenue for complaints resolution, the following matters fall outside its jurisdiction, excluding instances where the Ombud may refuse to investigate a complaint as per paragraphs 3.3.1.4 to 3.3.1.7 below:

3.3.1.1. The performance of functions by a military judge.

3.3.1.2. Matters pending before military or civilian courts.

3.3.1.3. Decisions already made by military or civilian courts.

3.3.1.4. The investigation risks undermining command channels or constituting insubordination in the Defence Force.

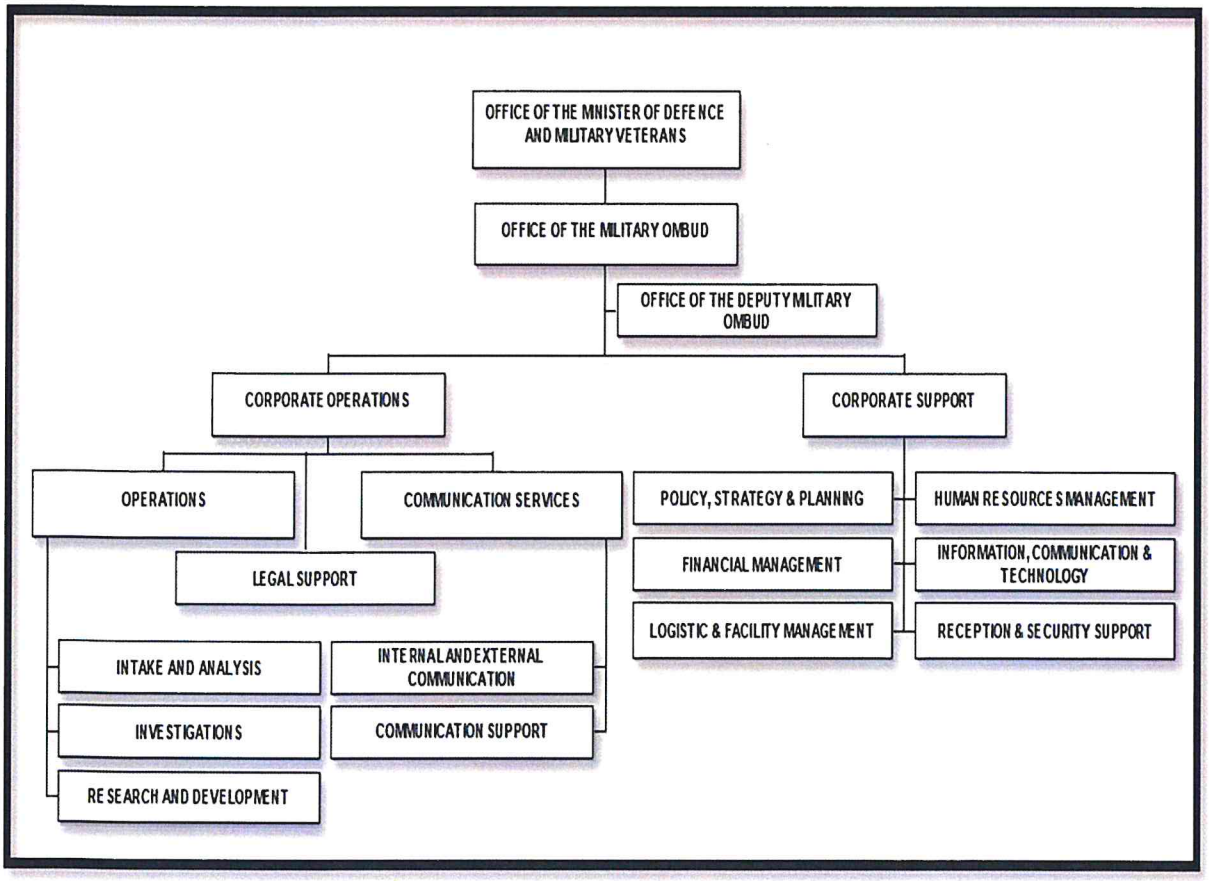
3.3.1.5. The complaint is frivolous or vexatious.

3.3.1.6. The complainant has failed to lodge a complaint within a reasonable time as prescribed.

3.3.1.7. The complainant has not first used mechanisms available under the Individual Grievances Regulations, 2016, unless the complaint pertains to systemic issues.

4. ORGANISATIONAL STRUCTURE OF THE OFFICE

4.1. The organisational structure of the Office as depicted below in **Figure 1**, is designed to ensure the efficient execution of its mandate, with clearly defined roles and responsibilities for key personnel.



5. GOVERNANCE STRUCTURES OF THE OFFICE

5.1. The governance structures of the Office are designed to ensure effective decision-making, accountability, and operational efficiency. The table below provides an overview of the hierarchical structure, illustrating the key governance bodies and their respective roles in the functioning of the Office.

Table 1: Governance Structures

Governance Structure	Function/Aim	Chairperson
a	b	c
Executive Committee Meeting (EXCO)	To provide strategic direction to the Office.	Military Ombud
Management Committee Meeting (MANCO)	To outline terms of reference for MANCO and develop an ongoing partnership/trust between Operations Chief Directorate, Legal Support Support, Executive Office and Corporate Support, enabling the organisational entities to co-ordinate efforts geared towards improved accountability, governance, risk and compliance for effective, efficient and transparent reporting.	Deputy Military Ombud
Military Ombud Dash-board (Operations)	To act as an oversight body ensuring standardisation and compliance to service delivery standards.	Military Ombud
Operations Manage-ment Meeting	The management and co-ordination of the Operations environments daily activities (i.e., assessment meetings and internal quality assurance meetings for complaints and investigation reports).	Chief Director Operations
Military Ombud Dash-board (Corporate Support)	The management and co-ordination of the Corporate Support environments daily activities.	Military Ombud
Corporate Support Management Meeting	The management and co-ordination of the Corporate Support environment daily activities.	Chief Corporate Support
Finance Governance Risk Compliance Sub-Committee	To ensure that the Office has accountable, transparent, cost-effective, efficient and equitable financial management.	Deputy Military Ombud
Human Resource Development Committee	To promote education, training and development within the organisation to enhance organisational performance.	Director Investigations

6. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF THE OFFICE

Table 2: Contact details

Title	Contact Details	
Contact Information for all PAIA Admin-Related Queries	Telephone:	+27 12 676 3800
	Toll Free:	+27 80 726 6238
	Facsimile:	+27 86 523 2296
	E-mail:	**paia@milombud.org**
Information Officer	Lieutenant General (Ret) V.R. Masondo	
Deputy Information Officer	Vacant	
Access to Information general contact details and other information		
Postal Address	SA Military Ombud Private Bag X163 Centurion Pretoria 0046	
Physical Address	Block C4 Eco Origin 349 Witch-Hazel Avenue Centurion Pretoria 0046	
Website	www.milombud.org	
Social Media	Find SA Military Ombud on Instagram, Facebook, @Mil_OmbudSA on X (Previously Twitter)	

7. DESCRIPTION OF THE SUBJECTS ON WHICH THE OFFICE HOLDS RECORDS; CATEGORIES OF RECORDS HELD BY THE OFFICE

Table 3: Description of Subjects of Records

Subjects on which the MO holds records	Categories of records held on each subject
OPERATIONS (Intake and Analysis; Investigations; Research and Development)	• Investigation Reports • Complaints Handling Manual • Complaints Master Register • Minutes of Meetings • Research Policy • Research strategy • Research papers • Surveys

CORPORATE SUPPORT (Financial Management; Human Resource Management; Policy, Strategy and Planning)	• Financial controls • Treasury Regulations • Finance Procedure Manual • MTEF guidelines • Tender documents
	• Guidelines on the recruitment and selection process in DPME • Job evaluation guide • Staff establishment • Finalised MO Investigation Reports • Bursary files • Selection records • Persol • Personal files of employees • Disciplinary records
	• Policies • Strategies • Strategic Plans • Annual Performance Plans • Annual Activity Reports • Quarterly Performance Reports • Security/Biometrics • Access Control Registers
COMMUNICATIONS	**Publicity and Marketing Material** • Banners • Posters • Outreach Programme • Outreach Attendance Registers • Brochures
	Publications • Military Ombud Act, 4 of 2012 • Military Ombud Complaints Regulations, 2015 • Communication and Marketing Strategy and Plan • Military Ombud Corporate Identity Manual • Military Ombud Newsletters • Frequently Asked Questions
	Media • Media Statements • Radio and TV Interviews • Printed Media Adverts • Social Media posts • Pictures/videos of staff and stakeholders • Internal Communications

	• Opinion Articles
LEGAL SUPPORT	**Legal Documents** • Legal Opinions • Litigation • Drafting and Review of Legal Documents • Memoranda of Understanding/Agreement • Service Level Agreements • National Preventive Mechanism Visit Reports

8. HOW TO REQUEST ACCESS TO RECORDS THAT ARE NOT AUTOMATICALLY AVAILABLE

8.1. Right of Access to Records

8.1.1. In terms of Section 11 of the PAIA, any person has the right of access to records held by the Office provided that:

8.1.1.1. The requester complies with all procedural requirements;

8.1.1.2. The record is required for the exercise or protection of any rights; and

8.1.1.3. Access is not refused on the grounds set out in Chapter 4 of PAIA.

8.2. How to Request Access to Records

8.2.1. A formal PAIA request is required for records not automatically available.

8.2.1.1. **Steps to Request Access to Records**:

8.2.1.1.1. A formal PAIA request is required for records not automatically available.

8.2.1.1.2. **Complete Form 2** – Request for Access to a Record. See details in footnote below.[2]

[2] To ensure efficient processing, the Requester must provide all the information required in Form 2, including, but not limited to:

- Full name and contact details (postal address, g, telephone number);
- Identification number (or company registration number, if applicable) (copy of identity document/card is required.);
- A clear description of the record(s) requested;
- Indication of the preferred format for receiving the record (electronic copy, hard copy, or in-person inspection);
- If requesting on behalf of another person, proof of authorisation (e.g., power of attorney); and

8.2.1.1.3. **Copy of Identity Card/Document** must be attached to the request form. Where the requester submits a request on behalf of another person, a copy of the latter's Identity Card/Document, as well as a written authority must be submitted. In the case of an attorney representing a client, a copy of the power of attorney must also be attached to the request form.

8.2.1.1.4. **Payment of request fee – submit proof of payment with completed request form.**

8.2.1.1.5. **Submit the form** *via* e-mail, post, or hand delivery.

8.2.1.1.6. **Processing Time**: **30** days (possible extension with notice).

8.2.1.2. **Submission Methods**:

8.2.1.2.1. The completed request form can be submitted *via*:

8.2.1.2.1.1. E-mail: paia@milombud.org;

8.2.1.2.1.2. **Postal Address:** SA Military Ombud, Private Bag, X163, Centurion, Pretoria, 0046;

8.2.1.2.1.3. **Hand Delivery:** Office of the Military Ombud, Block C4 Eco Origin,349 Witch-Hazel Avenue, Centurion, Pretoria, 0046

8.2.1.3. **Fees for Request Processing and Payment**:

8.2.1.3.1. In accordance with Section 22 of PAIA, the following fees may apply:

8.2.1.3.2. **Request fee:** Payable **before** processing begins;

- The right being exercised or protected (if applicable).

9. AUTOMATICALLY AVAILABLE RECORDS

9.1. Certain records as per a Notice filed with the Regulator are available **without a formal PAIA request having to be followed**, by means of the following methods:

9.1.1. **Website: www.milombud.org**

9.1.2. **E-mail Requests: paia@milombud.org**

9.1.3. **Telephonic & Postal Requests**: +27 80 726 6238 (Toll-Free): +27 12 676 3800; SA Military Ombud, Private Bag X 163, Centurion, Pretoria, 0046

9.1.4. **Physical Inspection**: Block C4, Eco Origin, 349 Witch-Hazel Avenue, Centurion, 0046

9.2. **Fees For Access**

9.2.1. Access to automatically available records is free of charge, except where prescribed fees apply for photocopying, printing, or postal delivery, as per the PAIA Regulations. **A fee schedule is available on request**.

10. DESCRIPTION OF ALL REMEDIES AVAILABLE IN RESPECT OF AN ACT OR A FAILURE TO ACT BY THE MILITARY OMBUD

10.1. Under the PAIA, requesters and other stakeholders have various remedies when the Military Ombud fails to act, refuses a request for access to information, or otherwise contravenes the provisions of the Act.

10.2. These remedies are the following **in hierarchical order**:

10.2.1. **Request Written Reasons** from the Military Ombud (Information Officer).

10.2.2. **Appeal to the Minister of Defence and Military Veterans** within **60** days. Form 4 (Lodging of An Internal Appeal) is available on request.

10.2.3. **Lodge a Complaint with the Regulator**. This option may only be exhausted after an internal appeal has unsuccessfully been lodged with the Minister.

10.2.4. **Application to Court**. If a requester is dissatisfied with the outcome of the complaint to the Regulator, or if no resolution is reached, the matter may be escalated to a competent Court of law for judicial review within 180 days.

8.2.1.3.3. **Access fee:** Payable if the request is granted and depends on the reproduction or search efforts required;

8.2.1.3.4. If the request is **voluminous**, a deposit of up to **one-third of the estimated access fee** may be required. **A fee schedule is available on request**.

8.2.1.3.5. **DOD Banking Details**: As the Office does not have self-accounting status, all payments iro a PAIA request must be made into the bank account of the DOD. The **DOD's bank details** are as follows:

Bank: ABSA Bank
Type of account: Cheque/Current
Branch Code: 632005
Beneficiary (Name of account holder): RSA Department of Defence
Beneficiary Account number: 1044280074
Deposit reference: Request fee

8.2.1.4. **Timeframe for Processing Requests**:

8.2.1.4.1. The Office will acknowledge receipt within **5** calendar days.

8.2.1.4.2. A decision on the request received must be made within **30** days from the date the request is received.

8.2.1.4.3. If an extension is needed (e.g., due to a high volume of requests or third-party consultations), the requester will be notified, stating the reasons.

8.2.1.5. **Decision on the Request**:

8.2.1.5.1. Upon evaluation, the Information Officer will:

8.2.1.5.1.1. **Approve the request**: The requester will be notified of any applicable access fees and how to obtain the records.

8.2.1.5.1.2. **Deny the request**: The requester will receive written reasons for refusal in terms of Chapter 4 of PAIA.

8.2.1.6. **Internal Appeal Process**:

8.2.1.6.1. If the requester is dissatisfied with the decision, an internal appeal may be lodged with the Minister within **60** days of the decision.

8.2.1.6.2. To lodge an appeal:

8.2.1.6.2.1. **Complete Form 4** - Internal Appeal Form (available on request).

8.2.1.6.2.2. **Submit it to the designated appeal authority** (Minister of Defence) along with supporting documents.

8.2.1.6.2.3. A **decision** on the appeal will be provided within **30** days.

8.2.1.7. **Further Remedies**:

8.2.1.7.1. If the internal appeal is unsuccessful, the requester may:

8.2.1.7.1.1. **Lodge a complaint** with the Regulator at: **PAIAComplaints@inforegulator.org.za** within **180** days.

8.2.1.7.1.2. **Apply to the Courts** within **180 days** from the final decision.

8.2.1.8. **Assistance to Requesters**:

8.2.1.8.1. In line with Section 19 of PAIA, the Information Officer must assist requesters free of charge who are illiterate, disabled, or unable to complete the request form.

8.2.1.8.2. To request assistance in the above regard, requesters must contact the Office as per the contact details provided in paragraph 6 above.

11. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

11.1. The Regulator has, in terms of Section 10(1) of PAIA, updated and made available the revised Guide on how to use it). The Guide is in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

11.2. The Guide is available in each of the official languages.

11.3. The aforesaid Guide contains the description of:

11.3.1. The objects of PAIA and POPIA;

11.3.2. The postal and street address, phone and fax number and, if available, electronic mail address of:

11.3.2.1. The Information Officer of every public body; and

11.3.2.2. Every Deputy Information Officer of every public and private body designated in terms of Section 17(1) of PAIA and Section 56 of POPIA.

11.3.3. The manner and form of a request for:

11.3.3.1. Access to a record of a public body contemplated in Section 11; and

11.3.3.2. Access to a record of a private body contemplated in Section 50.

11.3.4. The assistance available from:

11.3.4.1. The Information Officer of a public body in terms of PAIA and POPIA.

11.3.4.2. The Regulator in terms of PAIA and POPIA.

11.3.5. All remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging:

11.3.5.1. An internal appeal.

11.3.5.2. A complaint to the Regulator.

11.3.5.3. An application with a court against:

11.3.5.3.1. A decision by the Information Officer of a public body.

11.3.5.3.2. A decision on internal appeal.

11.3.5.3.3. A decision by the Regulator.

11.3.5.3.4. A decision of the head of a private body.

11.3.6. The provisions of:

11.3.6.1. Sections 14 and 51, requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual.

11.3.6.2. Sections 15 and 52 provide for the voluntary disclosure of categories of records by a public and private bodies, respectively.

11.3.6.3. Sections 22 and 54, regarding fees to be paid in relation to requests for access.

11.3.6.4. Section 92, regarding regulations made under PAIA.

11.4. **Accessing the Guide:**

11.4.1. Members of the public can inspect or make copies of the Guide from the offices of public or private bodies, including the office of the Regulator, during normal working hours.

11.4.2. The Guide can also be obtained as follows:

11.4.2.1. Upon request to the Information Officer or head of the private body, using Form 1, available at https://inforegulator.org.za/paia-forms;

11.4.2.2. Upon request to the Regulator, by sending Form 1 (a request for a copy of the Guide) to: **PAIACompliance@infoRegulator.org.za**;

11.4.2.3. From the website of the Regulator: https://inforegulator.org.za/paia-guidelines.

12. THE LATEST NOTICE REGARDING CATEGORIES OF RECORDS OF THE OFFICE WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

12.1. The Notice is available upon request as follows:

12.1.1. **Website: www.milombud.org**

12.1.2. **E-mail Requests: paia@milombud.org**

12.1.3. **Telephonic & Postal Requests**: +27 80 726 6238 (Toll-Free): +27 12 676 3800; SA Military Ombud, Private Bag X 163, Centurion, Pretoria, 0046

12.1.4. **Physical Inspection**: Block C4, Eco Origin, 349 Witch-Hazel Avenue, Centurion, 0046

13. SERVICES AVAILABLE TO MEMBERS OF THE PUBLIC FROM THE OFFICE AND HOW TO GAIN ACCESS TO THOSE SERVICES

13.1. **Lodging a Complaint with the Military Ombud**

13.1.1. In terms of Section 4(1)(*c*) of the Military Ombud Act, 4 of 2012, members of the public may lodge complaints with the Military Ombud regarding the official conduct of members of the Defence Force.

13.2. **Submission Requirements**

13.2.1. In accordance with Regulation 3 of the Military Ombud Complaints Regulations, 2015, all complaints must be submitted in writing using a form substantially similar to **Form 1 (Military Ombud Complaint Form)**, which is annexed to the Regulations as **Annexure "A"**. The complaint must include all relevant details to facilitate a fair and effective investigation.

13.2.2. Members of the public may use the following methods to lodge complaints with the Office:

13.2.2.1. **Phone Contact:**

13.2.2.1.1. Call the Office at the designated contact number.

13.2.2.1.2. Request to speak with an Intake Officer, who will provide guidance on how to complete and submit the complaint documentation.

13.2.2.2. **Physical Visit:**

13.2.2.2.1. Visit the Office in person.

13.2.2.2.2. Obtain a **copy of Form 1** and receive assistance from the Office staff regarding the complaint process.

13.2.2.3. **E-mail Request:**

13.2.2.3.1. Send an e-mail to the Office at **intake@milombud.org** to request a copy of Form 1.

13.2.2.3.2. The Office will provide the Form and any additional instructions required to complete the complaint process.

14. PUBLIC INVOLVEMENT IN THE FORMULATION OF POLICY OR THE EXERCISE OF POWERS OR PERFORMANCE OF DUTIES BY THE OFFICE

14.1. The Office is committed to fostering transparency, accountability, and inclusivity in the formulation of policies and the exercise of its powers and duties. As part of its mandate, the Office therefore actively engages with both military personnel and members of the public through various outreach and consultation initiatives. Below is an overview of the mechanisms used to involve the public:

14.2. **Outreach Programmes**:

14.2.1.1. **Engagement with Military Units**. The Office conducts regular outreach programmes at military units to educate members about the role of the Office, their rights, and the complaint process.

14.2.1.2. **Public Institution Outreach**. Similar programmes are extended to public institutions to create awareness of the Office's functions, the processes for lodging complaints regarding official conduct of members of the Defence Force, and collaboration between these Institutions and the Office.

14.2.1.3. **Public Consultation on Draft Military Ombud Legislation**:

14.2.1.3.1. When new legislation or amendments to existing legislation are proposed, notices

are published in government gazettes, newspapers, or other accessible platforms, allowing the public to review and provide inputs.

14.2.1.3.2. Members of the public, advocacy groups, and other stakeholders are encouraged to submit written comments or recommendations during the consultation period.

14.2.1.3.3. The Military Ombud carefully considers all public submissions to ensure policies and legislation reflect the needs and expectations of the broader community.

14.2.2. **Media Engagement**:

14.2.2.1. **Radio Interviews**. The Military Ombud actively participates in radio interviews to reach a wider audience. These interviews serve to:

14.2.2.1.1. Inform the public about the Ombud's mandate, complaint mechanisms, and rights under the Military Ombud Act, 4 of 2012.

14.2.2.1.2. Address frequently asked questions and promote the role of the Military Ombud in ensuring accountability within the Defence Force.

14.2.2.2. **Other Media Platforms**. The Office also engages with other media platforms, such as television, print, and social media, to disseminate critical information.

14.2.3. **Public Awareness Campaigns**:

14.2.3.1. The Office hosts and attends International Symposiums and Workshops related to the activities of Armed Forces Ombud Institutions.

14.2.3.2. The Office also distributes materials such as brochures, posters, and newsletters during outreach programmes and other public engagements.

14.2.4. **Regular Reporting and Transparency**:

14.2.4.1. The Office publishes annual reports detailing its activities, outreach programmes, and policy

developments. These reports are made accessible to the public.

14.2.4.2. The Office also reports annually to the Minister on its activities.

15. PROCESSING OF PERSONAL INFORMATION

15.1. The Office processes personal information in compliance with the Protection of Personal Information Act (POPIA), 4 of 2013, and its mandate under the Military Ombud Act, 4 of 2012. The processing of personal information is essential for the effective execution of the Office's duties, including:

15.1.1. **Complaints Handling**:

15.1.1.1. To investigate and resolve complaints lodged by Defence Force members, former members, or the public regarding official conduct.

15.1.1.2. To ensure accurate identification of complainants, respondents, and witnesses.

15.1.2. **Communication**:

15.1.2.1. To contact complainants, respondents, and other stakeholders during the complaint resolution process.

15.1.2.2. To provide updates on the status of investigations or responses to requests.

15.1.3. **Data Management**:

15.1.3.1. To maintain records for accountability, transparency, and compliance with legislative and reporting obligations.

15.1.3.2. To analyze data for the improvement of complaint handling processes.

15.1.4. **Legal and Policy Obligations**:

15.1.4.1. To comply with statutory and regulatory requirements related to access to information and the protection of personal data.

15.1.4.2. To fulfil obligations under PAIA and POPIA to safeguard the confidentiality, integrity, and availability of personal information.

15.1.4.3. The Office ensures that personal information is processed lawfully, securely, and only for purposes directly related to its functions.

16. DESCRIPTION OF THE CATEGORIES OF DATA SUBJECTS AND OF THE INFORMATION OR CATEGORIES OF INFORMATION RELATING THERETO

16.1. The processing of personal information by the Office is essential for:

16.1.1. **Complaint Resolution**: To investigate and resolve complaints in a fair and efficient manner.

16.1.2. **Communication**: To maintain contact with complainants, respondents, witnesses, and other stakeholders during investigations.

16.1.3. **Data Management**: To securely store and manage records for accountability, transparency, and compliance.

16.1.4. **Employment Administration**: To manage employee records, ensure compliance with employment laws, and support employee welfare.

16.1.5. **Legal Obligations**: To comply with statutory and regulatory requirements, including those under PAIA and POPIA.

Table 4: Categories of Data Subjects

Categories of Data Subjects	Personal Information that may be Processed
Natural Persons (Complainants; Witnesses and authorized representatives involved in complaints and investigations, Visitors to the Office).	Names and surname; contact details (contact number(s), fax number, e-mail address); Residential, postal or business address; Unique Identifier/Identity Number and confidential correspondence; Sensitive or private communications related to complaints or investigations.
Juristic Persons (Employers or institutions involved in complaints; Organizations/Entities providing legal or administrative support, Service Providers).	Names of contact persons; Name of legal entity; physical and postal addresses; contact details (contact number(s), fax number, e-mail address); registration number; financial, commercial, scientific or technical information and trade secrets.
Military Ombud Employees and their Family Members	Gender, pregnancy; marital status; race, language, educational information (qualifications); financial information; employment history; ID number; physical and postal address; contact details (contact number(s), fax number, e-mail address); criminal records; well-being of members,

Categories of Data Subjects	Personal Information that may be Processed
	medical, sex, nationality, ethnic or social origin, sexual orientation, age, physical or disability, religion, conscience, belief, culture, language, biometric information of the person.

16.2. **The recipients or categories of recipients to whom the personal information may be supplied**

Table 5: Categories of Personal Information

Category of Personal Information	Recipients or Categories of Recipients
Identity number and names, for criminal checks.	South African Police Services.
Educational qualifications.	South African Qualifications Authority, or any other approved Service Provider that conducts verification of educational qualifications.
Credit and payment history, for credit information.	Credit Bureaus.
Complainant and Respondent Information.	Relevant Defence Force authorities (e.g., C SANDF; Officers Commanding; Units, etc. involved in the complaint; Witnesses or other individuals involved in the complaint process (limited to necessary details). Courts of law, if personal information is required for legal proceedings; Other Oversight Bodies that the MO refers complaints to, as it falls in their legal and functional mandates).
Employee Information.	Administrative and legal compliance for employment purposes (e.g., Government departments, such as the Department of Defence or the Department of Labour, for reporting or compliance purposes; Payroll service providers for salary processing; Medical aid schemes or pension fund administrators for employee benefits management; Representative Trade Unions for membership purposes, contributions, etc.

16.3. **Planned transborder flows of personal information**. The Military Ombud has not planned transborder flows of personal information.

16.4. **General Description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the personal information held by the Office**

16.4.1. **Physical Security Measures**. The following measures are in place to safeguard personal information stored in physical form or accessed on-site:

16.4.1.1. **Access Control**:

16.4.1.1.1. Restricted physical access to the Head Office main building, offices, filing rooms, and servers.

16.4.1.1.2. Biometric and manual register access systems for authorized personnel only.

16.4.1.2. **Secure Storage**:

16.4.1.2.1. Personal information stored in locked filing cabinets or safes within secure areas.

16.4.1.3. **Surveillance Systems**:

16.4.1.3.1. CCTV cameras monitor and record access points to facilities.

16.4.2. **Technical Security Measures:** The following measures are in place to protect digital information from unauthorized access, alteration, or destruction:

16.4.2.1. **Secure Authentication:**

16.4.2.1.1. Strong password policies are enforced for system and database access.

16.4.2.2. **Firewalls and Intrusion Detection Systems (IDS):**

16.4.2.2.1. Firewalls monitor and block unauthorized access to networks.

16.4.2.2.2. IDS alerts the IT department of potential breaches or suspicious activities.

16.4.2.3. **Regular Backups**:

16.4.2.3.1. Daily, weekly, or monthly data backups are maintained as required, to ensure data availability in case of loss.

16.4.2.4. **Anti-Malware and Security Patches**:

16.4.2.4.1. Daily, weekly or monthly updates and patches as required, to software and systems to prevent vulnerabilities.

16.4.2.4.2. Antivirus software is installed and continuously updated to detect and block malicious activities.

16.4.3. **Data Lifecycle Management**. To ensure that information is managed securely throughout its lifecycle, the following measures are in place:

16.4.3.1. **Data Minimization**:

16.4.3.1.1. Personal information is collected and processed only for specific, legitimate purposes.

16.4.3.2. **Retention Policies**:

16.4.3.2.1. Personal information is retained only as long as necessary for operational or legal purposes.

16.4.3.2.2. Secure disposal methods, such as shredding or data wiping, are used to destroy obsolete information.

16.4.4. **Incident Response and Recovery**. The following measures are in place to mitigate the impact of potential security breaches:

16.4.4.1. **Incident Response Plan**:

16.4.4.1.1. A detailed response plan outlines steps to identify, contain, and mitigate breaches.

16.4.4.1.2. Immediate notification to affected individuals and regulatory authorities in the event of significant breaches.

16.4.4.2. **Disaster Recovery Plan**:

16.4.4.2.1. Contingency measures to ensure the continuity of operations during emergencies, such as power outages or cyberattacks.

16.4.4.3. **Testing and Updates**:

16.4.4.3.1. Regular testing of incident response and recovery plans to ensure their effectiveness.

16.4.5. **Monitoring and Evaluation**. The following are implemented to continuously improve security measures and adapt to emerging threats:

16.4.5.1. **Regular Security Assessments**:

16.4.5.1.1. Vulnerability assessments and penetration testing to identify and address weaknesses.

16.4.5.2. **Compliance Audits**:

16.4.5.2.1. Internal and external audits to ensure adherence to legal and regulatory requirements.

16.4.5.3. **Risk Management**:

16.4.5.3.1. Regular risk assessments to prioritize and address potential security threats.

17. AVAILABILITY OF THE MANUAL

17.1. This Manual will be made available in at least three official languages, and will be available as follows:

17.1.1. At the Office of the public body for public inspection during normal business hours;

17.1.2. To any person upon request and upon the payment of a reasonable prescribed fee; and

17.1.3. To the Regulator upon request.

17.2. **A fee** for a copy of the Manual, as contemplated in Annexure B of the Regulations, shall be payable per each A4-size photocopy made, as prescribed.

18. UPDATING OF THE MANUAL

18.1. The Office will review this Manual annually on the anniversary date of the Military Ombud's signature. However, a review may also be undertaken before the anniversary date should compelling reasons arise, such as changes in legislation, institutional developments, or directives from oversight bodies.

Issued by the Military Ombud