

# Protection of Personal Information Act (POPIA) Policy

**Al Anon Family Groups South Africa**

**Date approved:** 30 June 2026

**Review date:** 30 June 2026

**Version:** 1.0

---

## 1. Purpose of this Policy

The purpose of this policy is to ensure that **Al Anon Family Groups South Africa** complies with the Protection of Personal Information Act 4 of 2013 (“POPIA”) when processing personal information.

We are committed to protecting the privacy of our donors, beneficiaries, volunteers, staff, and partners, and to handling personal information responsibly and lawfully.

---

## 2. Scope

This policy applies to:

- All employees, volunteers, contractors, and board members.
  - All personal information processed by **Al Anon Family Groups South Africa**, regardless of format (paper or electronic).
- 

## 3. Definitions

**Personal Information** – Any information relating to an identifiable, living person (e.g., name, ID number, contact details, financial information).

**Processing** – Any activity involving personal information (collection, storage, use, sharing, destruction).

**Information Officer** – The person responsible for POPIA compliance within **Al Anon Family Groups South Africa**.

**Data Subject** – Any person whose personal information is processed by the organisation.

---

## 4. Roles and Responsibilities

- **Information Officer:** Mariette le Roux, Office Administrator, 021 595 4508
  - Ensures compliance with POPIA

- Handles requests from data subjects
    - Oversees training and awareness
  - **All Staff/Volunteers:** Must handle personal information in line with this policy.
- 

## 5. POPIA Conditions for Lawful Processing

We will:

1. **Be Accountable** – Assign responsibility and ensure compliance.
  2. **Limit Processing** – Only collect information that is necessary for our work.
  3. **Specify Purpose** – Clearly state why we collect the information and use it only for that purpose.
  4. **Further Processing Limitation** – Ensure any additional use is compatible with the original purpose.
  5. **Ensure Information Quality** – Keep information accurate, complete, and up to date.
  6. **Maintain Openness** – Inform individuals about what data we collect and how it will be used.
  7. **Apply Security Safeguards** – Protect personal information from loss, unauthorised access, or damage.
  8. **Enable Participation** – Allow individuals to access, correct, or delete their information.
- 

## 6. Consent

We will obtain voluntary, informed, and written (or electronic) consent before collecting personal information, except where collection is authorised by law or necessary for legitimate organisational purposes.

---

## 7. Data Subject Rights

Data subjects may:

- Request access to their personal information
  - Request correction or deletion of personal information
  - Withdraw consent
  - Lodge a complaint with the Information Regulator ([complaints.IR@justice.gov.za](mailto:complaints.IR@justice.gov.za))
- 

## 8. Security Safeguards

We will:

- Store physical records in locked cabinets with restricted access
  - Protect electronic records with strong passwords and encryption
  - Limit access to personal information to authorised personnel only
  - Securely destroy personal information when no longer required
- 

## **9. Retention and Destruction**

Personal information will be retained only as long as necessary for operational, legal, or archival purposes, after which it will be securely destroyed.

---

## **10. Sharing with Third Parties**

We will only share personal information with third parties where:

- It is necessary for our operations (e.g., service providers)
  - The third party has agreed in writing to comply with POPIA
  - The data subject has given consent or the law requires disclosure
- 

## **11. Training and Awareness**

All staff, volunteers, and board members will be trained on POPIA compliance and this policy at induction and annually thereafter.

---

## **12. Policy Review**

This policy will be reviewed annually or when there are material changes in POPIA, our operations, or best practices.

---

**Approved by: Ian Smit**

---

Name: Ian Smit

Position: Finance Chairperson  
Date: 30 June 2026

---

## **A. POPIA Consent Form**

**Al Anon Family Groups South Africa**  
**Date:** 30 June 2026

---

### **1. Purpose of this Form**

This form seeks your consent to allow **Al Anon Family Groups South Africa** to collect, store, and process your personal information in line with the Protection of Personal Information Act, 4 of 2013 (“POPIA”).

---

### **2. Personal Information Collected**

We may collect and process information including, but not limited to:

- Full name and surname
  - Identification number or date of birth
  - Contact details (phone, email, address)
  - Banking details (for donor debit orders or reimbursements)
  - Beneficiary details necessary for programme delivery
- 

### **3. Purpose of Collection**

Your personal information will be used for purposes including:

- Communicating with you about our activities, programmes, and opportunities
  - Processing donations and issuing Section 18A tax certificates
  - Managing your participation in our programmes or volunteer activities
  - Complying with legal and reporting obligations
- 

### **4. Security Measures**

We take all reasonable steps to protect your personal information from unauthorised access, disclosure, or loss.

---

## 5. Your Rights

You may request to:

- Access your personal information
  - Correct or update your information
  - Withdraw consent at any time
  - Lodge a complaint with the Information Regulator (complaints.IR@justice.gov.za)
- 

## 6. Declaration and Consent

I, \_\_\_\_\_ (full name), hereby consent to **Al Anon Family Groups South Africa** processing my personal information for the purposes stated above. I understand that my consent is voluntary and that I can withdraw it at any time in writing.

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

## B. POPIA Compliance Checklist

**Al Anon Family Groups South Africa**

**Prepared by:** Mariette le Roux

**Date:** 30 June 2026

| #  | Requirement                                                                        | Yes/No Notes/Actions |
|----|------------------------------------------------------------------------------------|----------------------|
| 1  | <b>Information Officer appointed and registered</b> with the Information Regulator |                      |
| 2  | <b>POPIA Policy adopted and communicated</b> to all staff/volunteers               |                      |
| 3  | <b>Consent forms</b> in place for donors, beneficiaries, and volunteers            |                      |
| 4  | <b>Privacy notices</b> included on website, forms, and communications              |                      |
| 5  | <b>Data inventory</b> completed – all personal information mapped                  |                      |
| 6  | <b>Purpose for collection</b> clearly recorded for each dataset                    |                      |
| 7  | <b>Access controls</b> in place (passwords, locked cabinets, role-based access)    |                      |
| 8  | <b>Third-party agreements</b> updated to include POPIA clauses                     |                      |
| 9  | <b>Retention schedule</b> developed and implemented                                |                      |
| 10 | <b>Secure destruction</b> process in place for outdated information                |                      |

| #  | Requirement                                                                    | Yes/No Notes/Actions |
|----|--------------------------------------------------------------------------------|----------------------|
| 11 | <b>Data subject request process</b> established (access, correction, deletion) |                      |
| 12 | <b>Incident response procedure</b> in place for data breaches                  |                      |
| 13 | <b>Annual staff training</b> completed and recorded                            |                      |
| 14 | Policy and procedures <b>reviewed annually</b>                                 |                      |

## C. Plain Language Privacy Notice

*(For website, email signatures, donor forms, event registrations, etc.)*

### Al Anon Family Groups South Africa – Privacy Notice

We value your privacy and are committed to protecting your personal information. When you share your details with us, we promise to:

1. **Use it only for the reason we collected it** – such as keeping in touch, processing donations, or providing services to you.
2. **Keep it safe** – we use secure systems, limit access to authorised staff, and will never sell your information.
3. **Be transparent** – you can ask us at any time what personal information we have about you and how we use it.
4. **Give you control** – you may update your details, withdraw consent, or request that we delete your information.

If you have any questions, contact our **Information Officer**:

**Name:** Mariette le Roux

**Email:** alanongso@alanon.org.za

**Phone:** 021 595 4508

If you believe we are not handling your personal information correctly, you can complain to the **Information Regulator**:

Email: complaints.IR@justice.gov.za

---

## D. Data Breach Response Template

### Al Anon Family Groups South Africa Data Breach Incident Response Plan

---

#### 1. Purpose

To outline the steps to follow if personal information is lost, stolen, or accessed without permission, in line with POPIA requirements.

---

## 2. Immediate Actions (Within 24 Hours)

1. **Identify & Contain** – Stop further loss or exposure (e.g., change passwords, disconnect affected systems).
  2. **Assess the Scope** – Determine what personal information was involved, how many people are affected, and how it happened.
  3. **Notify the Information Officer** immediately.
- 

## 3. Notification Requirements

The Information Officer must:

- Notify the **Information Regulator**
  - Notify **affected individuals** in plain language, including:
    - What happened
    - What personal information was affected
    - What the organisation is doing about it
    - What steps they can take to protect themselves
- 

## 4. Containment & Recovery

- Secure systems and restore data from backups if needed.
  - Update security measures to prevent recurrence.
- 

## 5. Investigation & Documentation

- Conduct an internal review to identify causes and prevention strategies.
  - Keep a written record of the incident, findings, and corrective actions taken.
- 

## 6. Post-Incident Review

- Review policies, procedures, and training needs.

- Report findings to the Board of Directors.

---

**Incident Report Form (to be completed for each breach):**

- Date/time of breach:
- Description of incident:
- Data involved:
- Number of individuals affected:
- Containment actions taken:
- Notifications made:
- Corrective actions planned: