



MEDIALENS INTELLIGENCE (PTY) LTD

POPIA POLICY

Internal policy for the lawful processing and protection of personal information.

Document version	1.0
Effective date	29 August 2026
Contact	paia@medialens.media
Status	Level 1 B-BBEE Contributor EME 100% Black-Owned Entity

This document should be reviewed by the appointed Information Officer before publication.

POPIA POLICY

1. Purpose and application

This policy establishes MediaLens Intelligence requirements for the lawful processing, protection, retention and management of personal information under POPIA. It applies to directors, employees, contractors, interns, consultants and third parties acting for MediaLens.

2. Governance and accountability

The Head of the private body is accountable for POPIA compliance. The Information Officer coordinates the compliance framework, handles requests and complaints, supports training, oversees assessments and monitors implementation. Contact: paia@medialens.media. The appointed Information Officer must be formally designated and registered with the Information Regulator before acting in that role.

3. Core rules for processing

- Process information lawfully, reasonably and only for a defined, legitimate business purpose.
- Collect only information that is adequate, relevant and not excessive for the purpose.
- Keep information accurate and allow appropriate correction.
- Use information only for the purpose communicated or another purpose permitted by POPIA.
- Apply safeguards proportionate to the sensitivity and risk of the information.
- Keep records only for the approved retention period, then securely delete, de-identify or archive them where lawful.

4. MediaLens processing activities

MediaLens may process client contacts, platform-user information, professional media-contact information, publicly available media references, client monitoring configurations, report data, customer-support communications, supplier records, employment information and website analytics. MediaLens must not treat publicly accessible information as free from POPIA obligations; staff must still use it lawfully, fairly and for a defined business purpose.

5. Roles and confidentiality

Access to personal information must be role-based and limited to those who need it. Staff must not export, share, screenshot, copy to private devices, sell, reuse or disclose client data, journalist databases, monitoring configurations, reports or licensed content unless authorised by the relevant contract, law or management approval. Confidentiality obligations continue after engagement ends.

6. Client data and operators

Where MediaLens processes personal information for a client, the applicable agreement must state the parties' roles, permitted purpose, confidentiality duties, security measures, sub-operator arrangements, retention/deletion requirements and incident-notification obligations. Operators engaged by MediaLens must be bound in writing to maintain appropriate safeguards and act only on MediaLens instructions.

7. Security safeguards

- Use strong passwords, multi-factor authentication where available and approved access controls.
- Store business data only in approved MediaLens systems and locations.

- Keep software, devices and access permissions current; remove access promptly when roles change or engagements end.
- Encrypt or otherwise protect sensitive information in transit and at rest where reasonably practicable.
- Maintain backups, audit logs and incident-response procedures appropriate to the service.
- Report suspected loss, unauthorised access, phishing, accidental disclosure or system compromise immediately to paia@medialens.media.

8. Data-subject requests and complaints

Requests for access, correction, deletion, objection or other privacy rights must be sent to paia@medialens.media and logged by the Information Officer. MediaLens must verify identity, assess the request, communicate the outcome within the applicable legal period and retain an audit trail. A data subject may complain to the Information Regulator if they believe their POPIA rights have been infringed.

9. Direct marketing and media contacts

Marketing by electronic communication must comply with POPIA, including consent and opt-out requirements where applicable. Professional media contacts must be used respectfully and only for relevant communications. Staff must honour opt-outs, correction requests and deletion requests that apply to MediaLens-controlled contact data.

10. Security compromises

On becoming aware of a suspected security compromise, staff must immediately preserve relevant information and notify the Information Officer. MediaLens will contain and assess the incident, take mitigation steps, document decisions and, where required, notify the Information Regulator and affected data subjects as soon as reasonably possible.

11. Training, monitoring and review

MediaLens will provide appropriate POPIA awareness training, review access permissions and data practices, maintain a compliance register and undertake privacy impact assessments when introducing or materially changing high-risk processing. This policy is reviewed annually and whenever services, law or processing practices materially change.

12. Approval and document control

Policy owner Information Officer / Head of Private Body

Approval authority N. Mteto

Effective date 29 August 2026

Review cycle Annual or after a material change

Contact paia@medialens.media

Before formal adoption, insert the registered entity/address details and confirm the Information Officer designation and registration. This policy supports compliance but should be reviewed against MediaLens' final systems, contracts and data flows.