Effective Date: 21 March 2026
Version: 3.2 (API-Approved Final)
Responsible Party: SOTAP (Pty) Ltd t/a AstraRed
Registration Number: k2019567615
Physical Address: 7 graphite rd
Email: privacy@astrared.co.za
WhatsApp: 072 118 5158

1. Introduction

AstraRed (“we”, “us”, “our”) operates a dual-platform that:

· Connects brands with influencers for performance-based campaigns (the Pod System), where influencers earn through recurring, measurable content creation.
· Provides a certified digital workforce that trains artificial intelligence (AI) models through on-device, privacy-preserving federated learning. Workers contribute by correcting or verifying AI outputs using their own mobile phones.

We are committed to protecting your personal information in accordance with the Protection of Personal Information Act, 2013 (POPIA) , the General Data Protection Regulation (GDPR) where applicable, and the platform policies of integrated services such as TikTok and Meta.

This Privacy Policy explains:

· What personal information we collect
· Why we collect it
· How we store, use, and share it

· Your rights and how to exercise them

By using our platform, you agree to the practices described in this policy.

2. Who We Are

Responsible Party: SOTAP (Pty) Ltd trading as AstraRed
Physical Address: 7 graphite rd
Email: privacy@astrared.co.za
Phone: 072 118 5158

2.1 Information Officers

We have appointed the following Information Officers in terms of POPIA and PAIA:

Role Name Contact
Information Officer Jesse T: 082 308 9107
Information Officer Richard A: 072 118 5158
Deputy Information Officer Oluchi A: 062 300 7515

3. Personal Information We Collect

[Content unchanged from previous version, but note: for workers who opt into AI training, we collect device-level usage data (battery, network status) only to control when training occurs, as described in Section 5.1.]

4. Use of Social Media Platform Data (TikTok, Meta, etc.)

AstraRed integrates with TikTok, Instagram, and Facebook through their official APIs. When you authorise such integration, we access only the data explicitly permitted by you via the OAuth consent screen, which typically includes:

· Public profile information (username, avatar)
· Email address
· Limited metadata and publicly available content strictly necessary for campaign verification (e.g., post URL, post ID, timestamp, and engagement metrics such as views, likes, and shares)

AstraRed does not download, store, or replicate media files (including videos, images, or audio) from social media platforms unless explicitly permitted by the platform and required for a specific, user-authorised function.

We do not:

· Access private messages or non-public communications
· Sell, transfer, or disclose platform-derived data to third parties
· Use platform data for surveillance or political targeting
· Combine platform-derived data with third-party datasets for profiling, enrichment, or resale
· Use platform-derived data for advertising targeting or audience building outside the respective platform ecosystems

Platform-derived data is used strictly for:

· Campaign verification
· Performance measurement
· Campaign matching and reporting

We store such data only as long as necessary and delete or anonymise it within 90 days after campaign completion or upon request.

4.1 Media Handling and Storage Limitations

AstraRed does not store, cache, or host raw media files (videos, images, or audio) obtained via platform APIs. Media is displayed via embedded links or platform APIs and remains hosted on the originating platform. Any temporary processing is strictly necessary, secure, and not retained beyond the processing session.

4.2 Scope of Platform Data Usage

Platform-derived data is used strictly for:

· Campaign verification
· Performance measurement
· Campaign matching and reporting

We do not use this data for:

· Advertising targeting or profiling
· Building unrelated user profiles
· Data enrichment, resale, or external aggregation

5. On-Device AI Training and Federated Learning (The “Worker”

Side)

AstraRed enables certified workers to contribute to AI model improvement through federated learning, a privacy-preserving technique where AI models are trained directly on users' devices without sending raw data to our servers.

5.1 How It Works

· Opt-in Consent: Workers must explicitly opt in to allow their device to participate. Consent is recorded with timestamp, IP, and consent version.
· User Controls: Workers can:
  · Enable or disable AI training at any time
  · Set training to occur only when the device is charging
  · Limit training to Wi-Fi only
  · Set a battery threshold (e.g., only train above 30%)
  · Schedule training during certain hours
· What Happens on the Device: When a worker makes corrections or verifies AI outputs, a small model update (gradients) is computed locally. No raw data ever leaves the device. Only the encrypted mathematical update is sent to our servers.
· Aggregation: The updates from many devices are combined to improve the global AI model. The process never reveals individual data.

5.2 Data Collected for This Feature

To enable these controls, we collect minimal device-level information only when the feature is active:

· Battery level (to enforce user-set limits)
· Network connection type (Wi-Fi vs. mobile data)
· Whether the device is charging
· A unique, non-personally-identifiable session identifier

This data is used solely to honour your preferences and is not stored beyond the session.

5.3 Your Consent

Before using AI training features, you will be presented with a clear, affirmative consent screen that explains:

· What the feature does
· That data never leaves your device
· Your control options
· That you can opt out at any time without affecting your ability to earn from other platform activities

You may withdraw consent at any time in the app settings.

6. The Pod System (Performance-Based Campaigns)

The Pod System is AstraRed's influencer offering. Brands create recurring content teams ("pods") where influencers post a specified number of times per month. Earnings are tied to performance (e.g., views, engagement) and are subject to the 70/30 revenue split (70% to influencer, 30% to AstraRed).

We collect the following information for this service:

· Campaign briefs and performance data
· Content submitted for approval
· Engagement metrics provided by social media platforms
· Payment records and invoicing details

All influencer data is processed in accordance with this policy and

used only for the purpose of fulfilling campaigns, measuring performance, and processing payments.

7. How We Use Your Information

[Same as previous version – table omitted for brevity but unchanged.]

8. Data Minimisation and Limitation

We collect only what is strictly necessary for the purposes described.

Platform Data Access Limitation: AstraRed requests only the minimum permissions required. We do not request access to private messages, contacts, or unrelated data.

9. Legal Basis for Processing

9.1 POPIA

· Consent
· Contractual necessity
· Legal obligation
· Legitimate interest

9.2 GDPR

Processing Activity Legal Basis
Account management Contract

Campaign execution Contract
Payments Contract
Identity verification Legal obligation
Fraud prevention Legitimate interest
Direct marketing Consent
Analytics Aggregated, anonymised internal analytics only (no profiling or resale)
On-device AI training Consent

10. Special Category Data

We process special categories of personal data only with explicit consent and for strictly necessary purposes:

· South African ID numbers – KYC, fraud prevention
· Biometric data (selfie) – identity verification, fraud prevention

This data is encrypted, stored securely, and used only for the stated purposes.

11. How We Store and Secure Your Information

11.1 Storage

· All data is stored on secure servers hosted by Amazon Web Services (AWS) in the Cape Town (af-south-1) region.
· Data is encrypted at rest using AES-256 and in transit using TLS 1.3.
· Access is restricted to authorised personnel with strict role-based controls.
· We maintain detailed audit logs of who accessed what, when,

and why.

11.2 Security Practices

· We align our security practices with ISO 27001 standards.
· We conduct regular vulnerability scans and penetration testing.
· We have a documented incident response plan with breach reporting procedures.
· All staff receive data protection and security training.

11.3 Data Retention

We retain personal information only as long as necessary for the purposes for which it was collected, or as required by law:

Data Type Retention Period
Active user accounts Duration of account + 1 year after deactivation
Inactive accounts 3 years after last activity
Financial records 5 years after last transaction (Tax Administration Act)
Consent records 5 years after consent is withdrawn
Campaign data 2 years after campaign completion
Platform-derived data 90 days after campaign/task ends, or until user disconnects
AI training contributions (encrypted updates) Not stored after aggregation; aggregated model stored indefinitely

After the retention period, data is securely deleted or anonymised.

12. Cross-Border Transfers

Your information is primarily stored in South Africa. Some

third-party operators (e.g., Stripe) may process data outside South Africa. Where such transfers occur, we ensure adequate protection through:

· Standard Contractual Clauses (SCCs) approved by the European Commission
· Binding corporate rules (where applicable)
· Adequacy decisions (where applicable)
· Written agreements containing GDPR-level safeguards

13. Cookies and Similar Technologies

We use cookies to improve your experience. Essential cookies are necessary for platform functionality; performance and targeting cookies require your consent. You can manage your cookie preferences through our cookie banner or your browser settings. For more information, see our [Cookie Policy] (link to be added).

14. How We Share Your Information

We only share your personal information in the following circumstances:

Recipient Purpose Safeguards
Businesses (for influencers) Campaign matching, content approval, payments Only necessary data; influencer consent via application
Influencers (for businesses) Campaign execution, communication Only necessary data; business must comply with platform policies
Third-party operators (AWS, Stripe, etc.) Hosting, payments, identity verification Data Processing Agreements (DPAs) in place,

including SCCs where required
Legal/regulatory authorities Compliance with POPIA, ARB, court orders As required by law
Acquirer (if business is sold) Transfer of assets Written agreement to protect your information

We never sell your personal information to third parties.

14.1 Subprocessors

Key subprocessors include:

· Amazon Web Services (AWS) – cloud hosting
· Stripe – payment processing
· VerifyNow – identity verification (if used)

All are bound by Data Processing Agreements.

15. Your Rights Under POPIA and GDPR

You have the following rights regarding your personal information:

Right Description How to Exercise
Access Obtain confirmation whether we hold your data and a copy of it Email privacy@astrared.co.za
Correction Correct inaccurate or incomplete data In-app profile update or email
Deletion Request deletion where processing is no longer justified Email or in-app “Delete Account” feature
Objection Object to processing for direct marketing or other legitimate interests Unsubscribe link or email
Withdraw consent Withdraw consent at any time (does not affect past processing) Email or in-app settings

Data portability Receive a structured, machine-readable copy of your data Email request

We will respond within 30 days (GDPR) or as soon as reasonably possible (POPIA).

Data Deletion Endpoint (for platform partners like TikTok and Meta):

Third-party platforms may call a dedicated endpoint to request user data deletion. We have implemented such an endpoint at: https://astrared.co.za/api/delete-user?platform={platform} &user_id={user_id}

For manual requests, users may use the in-app deletion feature or email privacy@astrared.co.za.

Platform Disconnection and Data Deletion: If a user disconnects a social media account:

· Access tokens are revoked immediately
· Data collection stops
· Platform-derived data is deleted within 30 days

Data Subject Request Verification: To protect user data, AstraRed may require identity verification before fulfilling any request related to access, correction, or deletion of personal information. This prevents unauthorised access or fraudulent requests.

You also have the right to lodge a complaint with the Information Regulator (South Africa) or the relevant EU supervisory authority.

16. Direct Marketing

We will only send marketing communications to you if you have given us explicit consent (opt-in). You may withdraw consent at any time by clicking the “unsubscribe” link in any marketing email or by contacting us.

We do not send marketing messages to influencers or workers without their separate consent.

17. Platform Role Clarity

AstraRed acts as:

· Data Controller when we determine the purposes and means of processing your personal information (e.g., account creation, fraud prevention, direct marketing).
· Data Processor when we process personal information on behalf of a business (e.g., influencer data used in a campaign). In such cases, the business remains the Data Controller and is responsible for ensuring its own legal basis for processing.

18. Automated Decision-Making and Profiling

We may use automated systems to assess:

· Fraud risk (e.g., detection of fake accounts or inauthentic engagement)
· Performance scores (for influencers and digital workers)
· Campaign matching recommendations

These automated decisions do not produce legal effects without

human review. If you disagree with an automated decision, you may request a manual review by contacting privacy@astrared.co.za.

19. API Compliance and Transparency

AstraRed complies with the data usage and platform policies of integrated services, including TikTok and Meta. We do not:

· Sell, transfer, or disclose platform-derived data to third parties
· Use platform data for surveillance, political targeting, or any purpose outside the scope of authorised campaign management
· Combine platform-derived data with third-party datasets for advertising profiling or resale

We maintain a clear audit trail of all data retrieved from platform APIs and regularly review our usage to ensure ongoing compliance.

We provide full transparency to platform providers during app review processes, including access to demonstration environments and clear documentation of how user data is collected, used, stored, and deleted.

API Abuse Prevention & Safeguards: We implement technical and organisational safeguards, including rate limiting, access monitoring, and anomaly detection, to prevent abuse of our systems and API integrations and to protect user data.

20. Data Breach Notification

If we discover a security compromise that is likely to affect your

personal information, we will:

· Notify the Information Regulator as soon as reasonably possible and, where required under applicable laws (including GDPR principles), within 72 hours of becoming aware of the breach
· Notify you directly (if required by law)
· Take steps to contain and remediate the breach

You will be informed of the nature of the breach, the potential consequences, and the measures we have taken.

21. User Responsibility

Users are responsible for ensuring that:

· They have the necessary rights, permissions, and consents for any content they upload or share
· Their use of AstraRed complies with applicable laws and platform rules

AstraRed is not responsible for user-submitted content that violates third-party rights.

22. Children's Information

Our services are not intended for individuals under the age of 18. We do not knowingly collect information from children. If you believe we have inadvertently collected data from a child, please contact us so we can delete it.

23. Global Standards Alignment

While AstraRed primarily operates under South African law, we align our data protection practices with internationally recognised standards to ensure a high level of security, transparency, and user trust.

24. Changes to This Privacy Policy

We may update this policy from time to time. The latest version will always be available at https://astrared.co.za/privacy. Material changes will be notified via email or platform announcement.

25. Contact Us

For any questions about this policy or to exercise your rights, please contact our Information Officer:

Email: support@astrared.co.za
Postal Address: 7 graphite rd
WhatsApp: 072 118 5158

You may also contact the Information Regulator directly using the details in Section 15.

AstraRed – Building a trusted, compliant digital workforce for South Africa.