PROTECTION OF PERSONAL INFORMATION POLICY

POPIA Privacy Policy

Company	NexBDM (Pty) Ltd
Registration	2026/250171/07
Version	1.2
Effective Date	25 May 2026
Previous Version	1.1 dated 24 May 2026
Next Review	21 November 2026
Information Officer	Heinoux Jakobus Roux
Classification	Public

PART A: INTRODUCTION AND OVERVIEW

1. WHO WE ARE

NexBDM (Pty) Ltd ("NexBDM," "we," "us," or "our") is a South African technology company registered in accordance with the Companies Act, No. 71 of 2008. We provide AI chatbot agent development, business automation consulting, SaaS platform services, and related technology services to businesses across South Africa.

Registered Name: NexBDM (Pty) Ltd

Registration Number: 2026/250171/07

Physical Address: 37 Montery Place, 140 Griffiths Road, Pretoria, Gauteng, 0184, South Africa

Website: www.nexbdm.co.za

Email: hjr@nexbdm.com

Phone: 079 607 5372

2. PURPOSE OF THIS POLICY

This Protection of Personal Information Policy describes what personal information NexBDM collects, why we collect it and how we use it, how we store and protect it, your rights as a data subject, how to exercise those rights, and how we handle third-party and client data.

3. OUR COMMITMENT

NexBDM is committed to processing personal information responsibly, lawfully, and in accordance with POPIA. We process personal information lawfully, fairly, and transparently, collect only what is necessary for a specific legitimate purpose, store information securely and only for as long as necessary, respect your rights as a data subject, and remain accountable for how we handle your information.

4. INFORMATION OFFICER

Name: Heinoux Jakobus Roux

Designation: Founder and Information Officer

Email: hjr@nexbdm.com

Phone: 079 607 5372

IO Registration Number: K2026250171

PART B: THE EIGHT CONDITIONS FOR LAWFUL PROCESSING

5. CONDITIONS FOR LAWFUL PROCESSING

Accountability: NexBDM is accountable for ensuring compliance with POPIA in all personal information processing activities.

Processing Limitation: We only collect personal information that is adequate, relevant, and not excessive for the purpose for which it is collected.

Purpose Specification: We collect personal information for specific, explicitly defined, and legitimate purposes.

Further Processing Limitation: Any further processing of personal information is compatible with the original purpose of collection.

Information Quality: We take reasonable steps to ensure the personal information we hold is accurate, complete, and up to date.

Openness: We maintain transparency about our processing activities through this Policy and our PAIA Manual.

Security Safeguards: We implement appropriate technical and organisational measures to protect personal information.

Data Subject Participation: We respect data subjects' rights to access, correct, and object to processing of their personal information.

PART C: WHAT PERSONAL INFORMATION WE COLLECT

6. CATEGORIES OF PERSONAL INFORMATION WE COLLECT

6.1 Prospective Client Information (Leads)

Identity information: Full name

Contact information: Email address, phone number, WhatsApp number

Business information: Business name, industry, number of employees, job title

Communication records: Notes from calls, emails, WhatsApp messages

6.2 Client Information

Identity and contact information: Full name, email, phone, physical address

Financial information: Invoice records, payment history

Contractual information: Signed SOW, NDA, change orders

Project records: Discovery session notes, process maps, solution designs, build documentation

6.3 SaaS Platform Users (NexSign, NexLog, NexCRM, NexSync)

Where NexBDM operates SaaS products, users who register for or use these platforms are data subjects in their own right. Information collected includes:

Account information: Full name, email address, organisation name

Authentication data: Hashed passwords, JWT session tokens (not stored in plain text), login timestamps

Usage data: Feature usage, audit logs, session duration, IP address at login

Billing contact: Name and email of the account owner for invoicing purposes (no card data stored by NexBDM)

SaaS platform users may exercise all rights under section 13 by contacting the Information Officer.

6.4 Client Customer Information (Operator Role)

When NexBDM builds chatbots or automation systems, we may process personal information belonging to our clients' customers. In this capacity NexBDM acts as Operator and will only process this data as instructed by the client (Responsible Party). A Data Processing Agreement governs this relationship.

6.5 Website Visitor Information

Technical information: IP address, browser type, device type

Usage information: Pages visited, time on site, referral source

Contact form submissions: Name, email, message content

7. HOW WE COLLECT PERSONAL INFORMATION

Directly from the data subject: Contact forms, email, WhatsApp, phone calls, discovery meetings

Indirectly: Google Ads leads, LinkedIn profiles, referrals

During service delivery: Access to client systems, data submitted by clients

Automatically: Website analytics, cookies, SaaS platform session tracking

PART D: WHY WE COLLECT PERSONAL INFORMATION

8. PURPOSES FOR PROCESSING

Prospective Clients: To qualify, assess fit, and prepare proposals. Lawful basis: Legitimate interest.

Clients: To deliver contracted services, manage the relationship, invoice, and collect payment. Lawful basis: Performance of a contract.

Clients' Customers (Operator): To build, test, and operate chatbots and automation as instructed by the client. Lawful basis: Performance of a contract between NexBDM and the client.

SaaS Platform Users: To provide, maintain, and improve SaaS platform functionality; to authenticate users and secure accounts; to process subscription billing. Lawful basis: Performance of a contract / Legitimate interest.

Suppliers and Contractors: To manage relationships and process payments. Lawful basis: Performance of a contract.

Website Visitors: To understand website usage and respond to enquiries. Lawful basis: Legitimate interest.

PART E: HOW WE STORE AND PROTECT PERSONAL INFORMATION

9. SECURITY SAFEGUARDS

Technical Measures

Access controls: Only the Information Officer has access to sensitive client data.

Password security: Strong, unique passwords and a password manager are used at all times.

Encrypted storage: Client credentials and sensitive data are stored in encrypted form.

HTTPS: The NexBDM website and all SaaS platforms use SSL/HTTPS encryption.

Infrastructure hardening: Following a security audit conducted in May 2026, NexBDM implemented server-level hardening measures including firewall rules, access key rotation, and deployment pipeline security controls on Hetzner/Coolify infrastructure.

JWT token security: Session tokens for SaaS platforms are short-lived, signed, and not stored in plain text. Token lifetimes are defined per platform (see section 12).

Organisational Measures

NDA requirements: All clients sign a Mutual NDA before any sensitive information is shared.

Data minimisation: Only the minimum information necessary is collected and retained.

Incident response: A data breach response process is documented in SOP_Compliance_DataBreachResponse.

10. THIRD-PARTY SERVICE PROVIDERS AND DATA SHARING

NexBDM uses third-party platforms to deliver its services and operate its SaaS products. Personal information may be processed by these platforms as sub-processors. NexBDM only shares personal information with third parties where necessary for service delivery and ensures appropriate contractual protections are in place.

Core Service Delivery

GoHighLevel CRM: Stores client contact and lead information. Hosted: USA.

n8n: Processes automation workflows which may include client data. Self-hosted on Hetzner (Germany).

Anthropic (Claude AI): Processes conversation data as part of chatbot solutions. Hosted: USA.

WhatsApp Business API: Facilitates client-facing messaging. Operated by Meta Platforms (USA).

Google Workspace: Email communication and document storage. Hosted: USA / EU.

Infrastructure and Hosting

Hetzner: Primary cloud infrastructure provider for NexBDM's self-hosted services and SaaS platforms. Servers located in Germany (EU). Subject to GDPR as well as POPIA contractual protections.

Coolify: Open-source self-hosted deployment platform running on Hetzner. No third-party data access. Managed by NexBDM's Information Officer.

Cloudflare: DNS, CDN, and DDoS protection for NexBDM domains. May process IP addresses and request metadata. Hosted: USA / Global. Cloudflare's data processing addendum is in place.

Cloudflare R2: Object storage used for file uploads and SaaS platform assets. Stored in Cloudflare's global network. No egress fees; data is encrypted at rest.

Payments

Paystack: Payment gateway for SaaS subscription billing. Processes payment card data on NexBDM's behalf. Paystack is PCI DSS compliant. Card data is NOT stored by NexBDM. Headquartered: Nigeria / USA.

Communications

Resend: Transactional email delivery for SaaS platform notifications (account creation, password reset, alerts). Processes recipient email addresses. Hosted: USA.

NexBDM does not sell personal information to third parties under any circumstances.

11. COOKIES AND WEBSITE TRACKING

The NexBDM website and SaaS platforms use cookies and similar tracking technologies. This section explains what types of cookies we use, why, and how you can control them.

11.1 Strictly Necessary Cookies

These cookies are essential for the website and SaaS platforms to function and cannot be switched off. They include session management cookies, security tokens, and load balancing cookies. No consent is required for these cookies as they are necessary to provide a service you have requested.

> Examples: login session cookies, CSRF protection tokens, JWT refresh cookies on NexSign/NexLog/NexCRM/NexSync.

11.2 Analytics and Performance Cookies

These cookies collect information about how visitors use our website, such as which pages are visited most often and whether error messages are received. All information is aggregated and anonymised. These cookies do not identify you personally.

> Platforms used: Google Analytics / similar. Legal basis: Legitimate interest with opt-out option.

You may opt out of analytics tracking at any time by adjusting your browser settings or using the opt-out mechanism on our website's cookie banner.

11.3 Non-Essential Cookies: Consent Requirement

NexBDM does not place non-essential cookies (marketing, retargeting, or third-party advertising cookies) without your prior, informed, and freely given consent, in accordance with POPIA section 11(1)(a) and the Information Regulator's guidance on online consent.

When you first visit the NexBDM website, a cookie consent banner will be displayed. You may accept all cookies, accept only necessary cookies, or customise your preferences. Your consent choice is recorded and stored. You may withdraw consent at any time by contacting us or clearing your browser cookies.

11.4 How to Manage Cookies

You may disable cookies in your browser settings at any time. Please note that disabling strictly necessary cookies may affect website and SaaS platform functionality, including your ability to log in.

12. RETENTION OF PERSONAL INFORMATION

NexBDM retains personal information only for as long as necessary to fulfil the purpose for which it was collected, to comply with legal obligations, or to resolve disputes.

12.1 Standard Retention Periods

Lead records not converted: 24 months from last interaction.

Client contractual records (SOW, NDA, invoices): 5 years from end of engagement.

Financial records (invoices, payments): 5 years.

Chatbot conversation logs: As specified in the client SOW (typically 12 months).

Website visitor data: 12 months.

12.2 SaaS Platform User Data

Active account data: Retained for the duration of the active subscription plus 90 days after cancellation or account closure, to allow data export.

Audit and usage logs: 12 months from date of creation, unless a longer period is required for security investigation or legal compliance.

Deleted account data: Purged within 30 days of account deletion, except where retention is required by law.

Billing records: 5 years from the date of the transaction (Companies Act / SARS requirement).

12.3 JWT Session Token Lifetimes

Short-lived session tokens are used across all NexBDM SaaS platforms. Tokens are not stored in plain text and are invalidated upon logout or expiry.

NexSign: Access token: 15 minutes. Refresh token: 7 days.

NexLog: Access token: 15 minutes. Refresh token: 7 days.

NexCRM: Access token: 30 minutes. Refresh token: 14 days.

NexSync: Access token: 15 minutes. Refresh token: 7 days.

If you believe a session token has been compromised, contact the Information Officer immediately to invalidate all active sessions for your account.

PART F: YOUR RIGHTS AS A DATA SUBJECT

13. YOUR RIGHTS UNDER POPIA

Right to access: Request confirmation of whether NexBDM holds your personal information and a copy thereof.

Right to correction: Request correction of inaccurate or outdated personal information.

Right to deletion: Request deletion where personal information is no longer necessary for the original purpose.

Right to object: Object to processing on grounds relating to your specific situation.

Right to lodge a complaint: Lodge a complaint with the Information Regulator of South Africa.

To exercise any of these rights, contact the Information Officer:

Email: hjr@nexbdm.com

Subject Line: POPIA Data Subject Request: [Your Name]: [Request Type]

Response Timeline: Within 30 days of receipt of your request

PART G: DATA BREACH AND INCIDENT RESPONSE

14. DATA BREACH MANAGEMENT

NexBDM maintains a documented Data Breach Response SOP (SOP_Compliance_DataBreachResponse). In the event of a breach the following steps apply:

STEP 1: Detect and contain the breach immediately.

STEP 2: Assess the nature, extent, and impact of the breach.

STEP 3: Notify the Information Regulator if the breach is likely to result in harm.

STEP 4: Notify affected data subjects as soon as reasonably possible.

STEP 5: Remediate the root cause and update security measures.

STEP 6: Document all breaches in the internal Breach Register.

PART H: CROSS-BORDER TRANSFERS

15. TRANSFER OF PERSONAL INFORMATION OUTSIDE SOUTH AFRICA

NexBDM transfers personal information to countries outside South Africa as required for service delivery. The following table sets out the known cross-border transfers and the basis on which they are made.

Recipient	Country	Data Transferred	Basis for Transfer
Hetzner	Germany (EU)	Infrastructure / hosted data	GDPR-compliant processor; contractual DPA in place
Google Workspace	USA / EU	Email, documents, analytics	Google DPA / Standard Contractual Clauses
GoHighLevel CRM	USA	Client and lead contact data	Contractual necessity; DPA in place with GHL
Anthropic (Claude)	USA	Chatbot conversation data	Contractual necessity; Anthropic DPA
Cloudflare	USA / Global	IP addresses, request logs	Cloudflare DPA; GDPR Standard Contractual Clauses
Paystack	Nigeria / USA	Billing email, payment metadata	PCI DSS compliance; Paystack DPA
Resend	USA	Recipient email addresses	Contractual necessity; Resend DPA
Meta (WhatsApp)	USA	Client messaging data	Contractual necessity; Meta Business Terms

NexBDM does not transfer personal information to countries that do not provide an adequate level of protection unless appropriate safeguards are in place, including Standard Contractual Clauses or binding corporate rules.

PART I: RELATED DOCUMENTS

16. RELATED POLICIES AND DOCUMENTS

PAIA Manual: POLICY_Compliance_PAIAManual_v1.1: Governs access to records held by NexBDM.

Data Breach Response SOP: SOP_Compliance_DataBreachResponse_v1.0: Governs incident response.

Record of Processing Activities: REGISTER_Compliance_ROPA_v1.0: Documents all processing activities.

IT Security Policy: POLICY_Compliance_ITSecurityPolicy_v1.0: Governs technical safeguards.

Terms of Service: POLICY_Legal_TermsOfService_v1.1: Governs service engagement with clients.

PART J: UPDATES AND CONTACT

17. UPDATES TO THIS POLICY

This Policy will be reviewed every 180 days and updated when there are material changes to NexBDM operations, processing activities, or applicable legislation. The current version is always available at www.nexbdm.co.za.

Version 1.0: 23 May 2026: Initial publication.

Version 1.1: 24 May 2026: Section numbering gaps resolved, third-party sharing section added, cookies section added, operator vs responsible party distinction clarified, related documents section added.

Version 1.2: 25 May 2026: Section 6 expanded to include SaaS platform user data (NexSign/NexLog/NexCRM/NexSync). Section 9 updated to reference May 2026 infrastructure security hardening and JWT token security. Section 10 expanded with Cloudflare, Hetzner, Coolify, Paystack, Resend, and R2 as named sub-processors. Section 11 fully restructured to comply with POPIA consent requirements for non-essential cookies (prior implicit consent replaced with explicit opt-in). Section 12 expanded with SaaS user data retention periods and per-platform JWT token lifetimes. Section 15 (cross-border transfers) replaced with named-provider table specifying transfer destination countries and contractual basis per provider.

18. CONTACT US

Information Officer: Heinoux Jakobus Roux
Company: NexBDM (Pty) Ltd
Email: hjr@nexbdm.com
Phone: 079 607 5372
Address: 37 Montery Place, 140 Griffiths Road, Pretoria, Gauteng, 0184, South Africa

If you are not satisfied with our response, you have the right to lodge a complaint with the Information Regulator of South Africa:

Email: complaints.IR@justice.gov.za
Website: www.inforegulator.org.za
Phone: 010 023 5200

AUTHORISATION AND SIGN-OFF

Effective Date: 25 May 2026
Name: Heinoux Jakobus Roux
Title: Founder and Director
Date Signed: 25 May 2026
Signature: 

DOCUMENT CONTROL

Version: 1.2
Effective Date: 25 May 2026
Previous Version: 1.1 dated 24 May 2026
Owner: Heinoux Jakobus Roux
Review Cycle: 180 days
Status: Active