



Privacy Policy

Public privacy policy for DeskFlow website, onboarding, clients and services

Version 2.2 | Effective 8 August 2026

Scope

This policy explains how DeskFlow handles personal information when it acts as a responsible party for its own business activities and, at a high level, how it handles information as an operator for client businesses.

1. Who we are

DeskFlow (Pty) Ltd is a South African business providing managed AI, automation and customer-management systems. Our registration number is 2026/460177/07. Our business address is 19 Kiaat Place, Amanzimtoti, Durban, KwaZulu-Natal, 4126, South Africa.

Privacy / Information Officer: Calvin Murray | calvin@deskflow.software. General contact: info@deskflow.software. Website: deskflow.software.

2. When this policy applies

This policy applies to personal information DeskFlow processes for its website, enquiries, sales, onboarding, client administration, telecom/phone-number verification, support, billing, security, compliance and service operations. It also explains our operator role when we process caller, customer or patient information on behalf of a client.

3. Our responsible-party and operator roles

- **DeskFlow as responsible party.** For our own website enquiries, prospective/client contacts, contracts, billing, support, security, supplier management and compliance records, DeskFlow generally determines why and how information is processed.
- **DeskFlow as operator.** For caller/customer/patient information processed to provide a client's DeskFlow service, the client generally determines the purpose of processing and DeskFlow generally processes the information on that client's instructions.

4. Personal information we may process

Context	Examples
Website and enquiries	Name, email, phone number, business/practice name, enquiry content, technical/browser information, referral/source information where available.
Client onboarding	Business/practice details, legal name, address, phone number, authorised representative name/contact/role, staff-access

Context	Examples
	details, notification email and setup information.
Telecom verification	Identity document and business-name/registration/address documents supplied by authorised representatives when required by a phone/telecom provider.
DeskFlow service for clients	Caller/customer name, phone number, caller type, reason for enquiry, potential urgency information, call/SMS metadata, SMS replies, AI summary/classification and transcript where enabled.
Support and platform use	User account details, support messages, tickets, configuration data, audit/security information and communications.
Billing and administration	Billing contacts, invoices, usage statements, payment status, accounting records and correspondence.

5. Health-related, special and children's information

Where DeskFlow supports a healthcare or orthodontic practice, callers may voluntarily disclose health-related information or information about a child. DeskFlow is configured to collect only the minimum enquiry information reasonably needed for the practice to follow up. DeskFlow does not provide clinical advice or make clinical decisions. The client practice remains responsible for the lawful processing of patient/child information and for its professional and healthcare obligations.

6. Why we process information

- to respond to enquiries and communicate with prospective or current clients;
- to create, configure, secure and support DeskFlow client accounts and services;
- to perform phone-number/telecom verification and related provider compliance;
- to provide AI receptionist, call recovery, CRM, messaging, workflow and follow-up functionality on behalf of clients;
- to send service notifications, support messages, usage statements, invoices and operational communications;
- to prevent fraud, abuse, unauthorised access and security incidents;
- to keep lawful business, tax, accounting, contractual, regulatory and dispute records; and
- to improve DeskFlow services using operational information that does not require using client caller/patient data for unrelated purposes.

7. Lawful processing

DeskFlow processes personal information only where there is a lawful basis under POPIA and other applicable law. Depending on the context, this may include consent, performance of a contract, compliance with a legal obligation, protection of a legitimate interest, or processing necessary for DeskFlow's or a third party's legitimate interests where permitted. Consent is used where the law specifically requires it, including certain direct-marketing situations.

8. AI and automated processing

DeskFlow may use AI to transcribe calls, summarise enquiries, classify call type or potential urgency, extract contact information, and trigger administrative workflows. AI outputs may be inaccurate. For healthcare clients, AI outputs are administrative aids only and must not be treated as diagnosis, clinical triage or medical advice. DeskFlow does not intentionally make solely automated clinical decisions about patients.

9. Who we may share information with

We may share personal information only as reasonably necessary with:

- the relevant client business/practice and its authorised users;
- our managed CRM, communications, telephony, AI, automation, email, hosting, document-storage, accounting and support providers;
- telecommunications or identity/business verification providers where required for phone-number compliance;
- professional advisers such as attorneys, accountants, auditors or security specialists; and
- regulators, law-enforcement bodies, courts or other persons where disclosure is required or permitted by law.

We do not sell patient/caller information or use client-controlled patient/caller information for unrelated DeskFlow marketing.

10. International / cross-border processing

Some technology providers may process or store information outside South Africa. Where DeskFlow is responsible for a transfer or facilitates a transfer as operator, we take reasonable steps to ensure the transfer is permitted under POPIA section 72 and is subject to appropriate safeguards or another permitted basis.

11. Security

DeskFlow uses reasonable technical and organisational measures designed to protect personal information from loss, damage, unauthorised destruction, unlawful access or unlawful processing. Measures include access controls, individual user access, multi-factor authentication where available, data-minimisation practices, controlled document handling, incident response procedures and supplier/security review. No online system can be guaranteed completely secure.

12. Retention and deletion

We keep personal information only for as long as reasonably necessary for the purpose for which it was collected, the active service relationship, support, legal/accounting requirements, security, disputes, provider backup cycles or an agreed retention period. Client-controlled service data is handled according to the client agreement and DPA. Verification documents are restricted and retained only as reasonably necessary for provider/regulatory evidence, audit, dispute or legal requirements.

13. Your rights

Subject to POPIA and applicable limitations, a data subject may request confirmation of whether we hold personal information, access to personal information, correction or deletion of inaccurate/unlawfully held information, or object to certain processing. A person may also withdraw consent where processing depends on consent.

Where a request concerns information that DeskFlow processes only on behalf of a client, we may refer the request to that client as the responsible party. We may ask for information necessary to verify identity or authority before acting on a request.

14. Direct marketing

DeskFlow will follow applicable POPIA requirements for direct marketing by electronic communications. Marketing messages will provide a reasonable way to opt out where required. Service, billing, security and operational communications are not treated as optional marketing merely because they are electronic.

15. Cookies and website analytics

Our website may use essential cookies or similar technologies needed for security and core functionality. If we enable non-essential analytics, advertising or similar cookies that require consent, we will provide an appropriate consent choice and update this policy or a cookie notice with relevant details.

16. Security compromises

If DeskFlow identifies a security compromise involving personal information for which DeskFlow is the responsible party, DeskFlow will take reasonable steps to investigate, contain and make notifications required by law. If the affected information is controlled by a client and DeskFlow is acting as operator, DeskFlow will notify the client in accordance with the DPA so the client can meet its responsible-party obligations.

17. Complaints and contact

Privacy requests and complaints may be sent to Calvin Murray, Information Officer, at calvin@deskflow.software. General enquiries may be sent to info@deskflow.software.

You may also lodge a POPIA complaint with the Information Regulator (South Africa). Current Regulator contact details published at the effective date of this policy include: Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191; telephone 010 023 5200; toll-free 0800 017 160; general email enquiries@inforegulator.org.za; POPIA complaints: POPIAComplaints@inforegulator.org.za.

18. Changes to this policy

We may update this Privacy Policy as our services, providers or legal obligations change. The current version will be published on the DeskFlow website with an effective date.