



POPIA Operator & Data Processing Addendum

Written operator terms for processing personal information on behalf of DeskFlow clients

Version 2.2 | Effective 8 August 2026

Why this document exists

POPIA requires a responsible party to use a written contract to ensure that an operator processing personal information establishes and maintains appropriate security measures. This Addendum records DeskFlow's operator obligations and the Client's responsible-party instructions.

1. Parties, scope and legal roles

This POPIA Operator & Data Processing Addendum (DPA) forms part of the Managed Services & Trial Agreement between DeskFlow (Pty) Ltd (DeskFlow) and the Client identified in DeskFlow onboarding.

For customer, caller or patient information processed to provide the Client's services, the Client generally determines the purpose and means of processing and therefore generally acts as the responsible party under POPIA. DeskFlow generally acts as an operator to the extent it processes that information on the Client's documented instructions.

DeskFlow acts as a separate responsible party for personal information it processes for its own legitimate business administration, including client contracting, billing, support, supplier management, security, legal compliance and website enquiries.

2. Subject matter, duration and purpose

Item	Description
Subject matter	Provision of DeskFlow managed CRM, AI receptionist, call/SMS recovery, workflows, communications, reporting, support and related enabled services.
Duration	For the active trial/subscription and any limited post-termination period reasonably required for export, return, deletion, backups, legal compliance, billing or disputes.
Purpose	Capture, transmit, organise, summarise, classify and present customer/caller enquiry information to the Client; operate enabled communications and workflows; provide support; maintain service security and records.
Processing operations	Collection, receipt, recording, organisation, storage, retrieval, consultation, transmission, summarisation, classification, restriction, export and deletion, depending on enabled features.

3. Data subjects and categories of personal information

Data subjects	Typical information
Client representatives and staff	Name, work contact details, role, login/user information, support communications, onboarding information.
Prospective and existing customers/callers	Name, phone number, email where provided, enquiry reason, SMS replies, call metadata, communication history, AI-generated summary/classification.
Healthcare callers/patients/parents or guardians	Limited enquiry context that may include health-related information voluntarily disclosed by the caller, potential urgency wording, and relationship to the patient.
Authorised representative for telecom verification	Name, contact information, role/capacity, identity document and business verification documents supplied for regulatory/provider verification.

DeskFlow is configured to minimise unnecessary collection. For healthcare launch configurations, DeskFlow does not intentionally request national ID numbers, medical-aid details, payment-card details, full medical histories, detailed treatment records, extensive symptoms or preferred callback times unless a later lawful use case is separately approved and configured.

4. Special personal information and children

Some healthcare enquiry content may constitute special personal information, including health information, and some enquiries may relate to children. The Client is responsible for identifying and maintaining a lawful basis/authorisation for that processing, including any obligations applicable to health information or children's information. DeskFlow will process such information only to the extent it is received or necessary for the instructed service and will not use it for unrelated purposes.

5. Client instructions and responsibilities

- The Client instructs DeskFlow to process personal information only for the enabled DeskFlow services and related support/security/compliance functions described in the Agreement and onboarding submission.
- The Client is responsible for the lawfulness, accuracy and fairness of its instructions, notices, collection practices, customer/patient relationships and use of the resulting information.
- The Client will not instruct DeskFlow to process information unlawfully or for prohibited purposes.
- The Client will limit user access to authorised staff and promptly request access changes when roles change.
- The Client will provide or approve required privacy notices, call/SMS wording and lawful communication practices for its data subjects.

6. DeskFlow operator obligations

- Process personal information only with the Client's knowledge/authorisation and for the proper performance of the services, unless required otherwise by law.
- Treat personal information as confidential and limit access to persons who need it for authorised duties.
- Maintain appropriate and reasonable technical and organisational safeguards having regard to the risks, the nature of the information and generally accepted security practices.
- Assist the Client, within reasonable limits, with data-subject requests, security incidents, information needed for compliance assessments and other POPIA obligations relevant to DeskFlow's processing.
- Keep reasonable records of material operator processing and supplier/subprocessor arrangements.
- Not sell Client caller/patient information, add it to unrelated marketing lists, or use it for DeskFlow marketing.

7. Security measures

DeskFlow will apply reasonable safeguards proportionate to a small managed service provider and the systems used. Measures may include:

- separate client sub-accounts/workspaces where supported;
- role-based/restricted user access and individual staff logins;
- multi-factor authentication where available and appropriate;
- strong account and device-security practices;

- limited collection and configuration designed to reduce unnecessary health/sensitive information;
- call recording disabled by default for healthcare launch use;
- controlled handling of identity/business verification documents;
- workflow, prompt and notification testing before live activation;
- incident response, access review, supplier review, retention/deletion and offboarding procedures; and
- reasonable backups, monitoring and recovery practices available through DeskFlow or its service providers.

No security system can guarantee absolute security. Each party must promptly address known weaknesses within its control.

8. Security compromises

Where DeskFlow has reasonable grounds to believe that Client personal information has been accessed or acquired by an unauthorised person, DeskFlow will notify the Client immediately after DeskFlow has sufficient information to identify a credible incident, and will provide available information reasonably needed for the Client to assess and meet its responsible-party obligations. DeskFlow will take reasonable steps to contain, investigate and mitigate the incident.

Unless DeskFlow is independently the responsible party for the affected processing, the Client remains responsible for determining and making notifications to the Information Regulator and affected data subjects under POPIA. DeskFlow will reasonably assist.

9. Subprocessors and service providers

The Client gives general authorisation for DeskFlow to use subprocessors/service providers reasonably necessary to deliver the enabled service, subject to appropriate confidentiality, security and data-protection terms where reasonably available. DeskFlow remains responsible for managing those providers within the scope of its contractual relationship with them.

DeskFlow may replace or add providers as the service evolves. Where a change is reasonably likely to materially affect privacy/security risk for active Client data, DeskFlow will provide reasonable notice where practical.

10. Cross-border processing

Some cloud, AI, communication, support or infrastructure providers may process or store personal information outside South Africa. Where DeskFlow makes or facilitates a cross-border transfer, it will take reasonable steps to ensure the transfer is permitted under POPIA section 72, including through applicable law, contractual safeguards, binding rules, consent or another legally permitted basis as appropriate.

The Client authorises cross-border processing necessary for the enabled DeskFlow service subject to these safeguards and may request reasonable information about the applicable provider categories.

11. Data-subject and PAIA requests

If DeskFlow receives a request concerning Client-controlled caller/customer/patient information (for example access, correction, deletion or objection), DeskFlow will, where appropriate, refer the request to the Client and will not independently alter Client-controlled records except on Client instruction or where law requires. The Client is responsible for the substantive response as responsible party. DeskFlow may verify identity/authority before disclosing or changing information.

12. Retention, return, export and deletion

- DeskFlow will not intentionally keep Client personal information longer than reasonably necessary for the active service, support, lawful record-keeping, security, billing, disputes, backups or an agreed retention period.
- On termination, DeskFlow may provide a reasonable export/return opportunity where supported and authorised.
- After the applicable offboarding period, DeskFlow may delete or de-identify Client personal information from active systems, subject to provider backup cycles and records that must lawfully be retained.
- The Client should export any information it needs before access is finally disabled.
- Identity/business verification records will be restricted and retained only as reasonably necessary for telecom/provider verification, audit, dispute or legal obligations.

13. Audit and information

On reasonable written request, DeskFlow will provide information reasonably necessary to demonstrate compliance with this DPA, subject to confidentiality, security, third-party restrictions and proportionality. Formal on-site audits are not included in standard pricing and may be subject to reasonable scope, timing, confidentiality and cost arrangements unless required by law or a regulator.

14. Liability and precedence

Liability under this DPA is subject to the liability framework in the Managed Services & Trial Agreement except to the extent a limitation is prohibited by law. If this DPA conflicts with the main Agreement on the handling of Client personal information, this DPA controls for that processing matter.

15. Electronic acceptance

The Client accepts this DPA when its authorised representative electronically accepts the DeskFlow legal terms during onboarding or signs a client-specific order that incorporates this DPA.

Schedule A - Current subprocessor categories

Provider / category	Purpose	Typical data
HighLevel / LeadConnector and related platform infrastructure	Managed CRM, workflows, conversations, Voice AI/telephony integrations, SMS/email automation, reporting and account access.	Client setup information, contacts, call/SMS records, transcripts/summaries where enabled, communications and workflow data.
Telecommunications / messaging carriers used through the platform	Phone numbers, call routing, voice, SMS and related delivery.	Phone numbers, call metadata, message content and related routing information.
Business email / domain providers	DeskFlow business email, notifications and client communications.	Sender/recipient information, email content and attachments where used.
Accounting / billing systems	Invoices, usage statements, payment administration and bookkeeping.	Client business/billing contacts, invoices, payment status and accounting records.
Cloud hosting / document storage providers	Website/application hosting and secure storage of business or compliance records where used.	Client onboarding data, contracts or support records depending on the system.
Professional advisers	Legal, accounting, compliance or security advice where necessary.	Limited information necessary for the specific professional purpose.

DeskFlow maintains a supplier/subprocessor register and may update provider names as its infrastructure changes. A current category-level list can be requested at info@deskflow.software.

Legal basis referenced

This DPA is structured with particular regard to the Protection of Personal Information Act 4 of 2013 (POPIA), including sections 19 to 22 (security safeguards and operator processing) and section 72 (transborder information flows).