

1. Introduction

OpShifts (Pty) Ltd ("OpShifts," "we," "us," "our") provides a WhatsApp-based workforce management platform for hospitality venues in South Africa. This policy explains how we collect, use, store, and protect personal information, in line with the Protection of Personal Information Act 4 of 2013 ("POPIA").

This policy applies to two distinct groups of people, treated differently below because POPIA treats them differently:

- Venue account holders (managers/owners who sign up for OpShifts) — for this group, OpShifts is the "responsible party" under POPIA.
- Staff members (employees of a venue using OpShifts to manage their shifts) — at their first WhatsApp interaction, staff members receive a privacy notice stating that the venue is the "responsible party" and OpShifts is the "operator" processing staff data on the venue's instruction. The venue confirms that it has lawful authority to provide staff members' personal information to OpShifts and to instruct OpShifts to process it. Staff members with questions about their data should contact their employer (the venue) first; we process their information under the venue's instruction, not our own independent purpose.

2. Information Officer

OpShifts' Information Officer:
Cameron Torrance
Email: cameron@opshifts.com

3. What Personal Information We Collect

From venue account holders (managers/owners):

- Full name, email address, phone number
- Business/venue name, address, and CIPC registration details — collected to verify the venue is a legitimately registered business, for billing/invoicing purposes, and to ensure any agreement between OpShifts and the venue is with a real, identifiable legal entity
- Billing information (processed via Paystack)
- Login/PIN credentials for dashboard access
- Venue configuration and operational settings — operating hours, staffing rules, automation preferences, staffing ratios, and similar business configuration data entered by the venue to run the platform

From staff members, on behalf of venues:

- Full name and phone number (WhatsApp number)
- Role, department, employment type, experience level, skills
- Shift availability, preferences, and history
- Leave, shift swap, and time-off requests

On health information specifically: OpShifts does not collect a free-text "reason" field on any staff request type (sick day, leave, day-off, or shift swap) — every request flow is designed to capture only what's operationally necessary (the request type, dates, and shift affected), with no open text field where a staff member could volunteer detailed health or medical information. For sick leave, OpShifts processes this information only on the venue's documented instructions.

A distinction worth being precise about: OpShifts' product does include a "sick day" request type as distinct from leave, swap, or day-off — meaning the fact that an absence was sick-leave-related is inherent to the product, not something removing the reason field changes. This categorization is processed by OpShifts only on the venue's documented instructions and solely as necessary to administer sick leave entitlements under South African labour law. What OpShifts avoids entirely, by design, is any detailed or diagnostic health information — specific conditions, symptoms, or medical detail — which the removal of all free-text reason fields is specifically intended to prevent.

Doctor's note policy reminders (optional, per-venue): On the venue's documented instructions, OpShifts may send an automated WhatsApp reminder to staff who report sick leave meeting a venue-configured threshold (e.g. after a set number of consecutive sick days), reminding them of the venue's own sick-note policy. The note itself is never collected, transmitted, or stored by OpShifts — it remains an entirely offline matter between staff and their employer, exactly as it would without OpShifts involved. OpShifts' role is limited to sending the policy reminder and, optionally, letting a manager record a simple yes/no administrative flag ("note received") authorized by the venue as necessary to administer employment leave — never the document or its contents.

If a staff member voluntarily discloses health-related details anyway (despite not being asked and against the design of the flow), OpShifts will apply the same reasonable security measures to that information as to all other personal information it holds. However, OpShifts is not responsible for a staff member's decision to disclose health information it did not request, and disclaims liability arising specifically from that unsolicited disclosure, to the fullest extent permitted by law.

4. How We Collect Information

- Directly from venue managers during account sign-up (Retool dashboard)
- Directly from staff members via WhatsApp
- From venue managers entering or updating staff details on their behalf

5. Why We Process This Information

- Venue account details — used for account creation, service provision, and billing
- Staff names, roles, skills — used for accurate, fair, legally compliant rostering
- Availability, leave, sick day requests — used for staff self-management, so managers avoid manual chasing
- WhatsApp phone numbers — the core mechanism for the staff-facing product
- Billing information — used for monthly subscription processing via Paystack

We do not process personal information for any purpose beyond running the OpShifts service. Data is never sold, and never used for advertising or profiling unrelated to workforce scheduling.

6. Who We Share Information With

- Meta (WhatsApp Business Platform) — processes staff WhatsApp messages and phone numbers. Located globally. Legal basis for cross-border transfer: consent (given at first WhatsApp interaction).
- Supabase — processes all staff, roster, and venue data. Located in Frankfurt, Germany. Legal basis for cross-border transfer: EU data protection standards generally recognized as adequate.
- Make.com — processes automation connecting WhatsApp to our database. EU-based. Legal basis for cross-border transfer: as above.
- Retool — hosts the manager dashboard. Located in the United States. Legal basis for cross-border transfer: consent (given at account sign-up) and a fully executed Data Processing Agreement incorporating enforceable safeguards that provide an adequate level of protection for personal information (DocuSign Envelope 20981A64-BA54-4F5A-BDA5-37AB043D1D06).
- Paystack — processes billing and payment information. Located in South Africa (Paystack also operates across other African markets). Paystack maintains an operational physical presence in South Africa, with a local office located in Cape Town.

We never sell personal information to third parties. Each venue's staff data is isolated from every other venue's data — confirmed at the application level, with database-level Row-Level Security enforcement completed before any pilot venue's real staff data enters the system.

7. AI-Assisted Processing and Scheduling

OpShifts may use a third-party AI service, on the venue's documented instructions, to convert staff members' free-text availability messages into structured scheduling information, such as dates, shifts, and availability periods. We limit information shared with the AI service to what is

reasonably necessary for that function and require the provider to process it only on our instructions and not to use it to train or improve general-purpose AI models.

The AI service is not used to engage in open-ended conversations with staff, generate responses to staff, approve or reject requests, or make final employment, rostering, leave, disciplinary, pay, or other consequential decisions. Staff should not include health or other sensitive personal information in free-text availability messages; OpShifts does not use such information as an input to AI-assisted scheduling recommendations.

OpShifts may in future provide authorised venue managers with AI-assisted scheduling recommendations based on relevant operational information, such as availability, role, skills, hours worked, and venue-configured staffing requirements. Any such recommendation will be subject to review and approval by an authorised venue manager, who may reject, amend, or override it and remains responsible for the final decision. OpShifts will provide reasonable mechanisms for venues and staff members, through the venue, to identify and correct inaccurate scheduling information used for these purposes.

8. Data Retention

- Active accounts: staff members' data is retained for the duration of the venue's active subscription, in accordance with the venue's documented instructions and applicable employment-record retention obligations.
- After a venue cancels: staff members' data is retained for 90 days (allowing reactivation or data export), after which OpShifts deletes it, unless the venue instructs otherwise or retention is required by law.
- Individual staff members who leave a venue's employment: their data is removed or anonymized within 12 months of being marked inactive, unless the venue instructs otherwise or retention is required by applicable employment-record retention obligations.
- WhatsApp conversation logs: retained for 12 months on a rolling basis, then purged, unless the venue instructs otherwise or retention is required by law.

9. Security Measures

We take reasonable technical and organisational measures to protect personal information, including:

- Encrypted data transmission (HTTPS/TLS) across the platform
- Row-Level Security enforced at the database level, isolating each venue's data from every other venue's
- Access-controlled manager dashboard login
- Staff data visibility limited to the relevant venue only

10. Your Rights Under POPIA

You have the right to:

- Be informed that your personal information is being collected and why
- Access the personal information we hold about you
- Request correction of inaccurate or outdated information
- Request deletion, subject to legal retention requirements
- Object to processing in certain circumstances
- Complain to the Information Regulator

Staff members: requests to access, correct, or delete your information should generally go to your employer (the venue) first, as the responsible party for your data. We support venues in fulfilling these requests as their operator.

To contact us directly: cameron@opshifts.com

To complain to the Information Regulator:

Email: complaints.IR@justice.gov.za

Website: inforegulator.org.za

11. Data Isolation Between Venues

Each venue's staff data is kept fully separate from every other venue's — enforced both in the application and at the database level. Staff and managers at one venue cannot access or view data belonging to another venue.

12. Children & Minimum Working Age

OpShifts relies on venues to comply with the Basic Conditions of Employment Act's minimum working age and youth employment restrictions. Each venue remains solely responsible for all employment decisions, rostering decisions, compliance with labour laws, and the accuracy and lawfulness of staff information and instructions supplied through OpShifts. OpShifts does not independently verify staff age and has no visibility into a staff member's age beyond what a venue chooses to record — this responsibility sits with the employer, not with OpShifts.

13. Data Breach Notification

In the event of a security compromise involving staff personal information, OpShifts will promptly notify and assist the venue, including by providing a description of the breach, its likely consequences, and remedial steps being taken. The venue will notify affected staff members and the Information Regulator as soon as reasonably possible, unless applicable law requires OpShifts to notify directly — in line with POPIA's breach notification requirements.

14. Changes to This Policy

We may update this policy from time to time. Material changes will be communicated to venue account holders via email or dashboard notice.

15. Contact Us

OpShifts (Pty) Ltd

Information Officer: Cameron Torrance

Email: cameron@opshifts.com