LABOURDRIVE

POPIA COMPLIANCE & DATA PROTECTION POLICY

Internal governance and external assurance framework

Effective date: 01 October 2026

This policy may be updated from time to time & is therefore subject to amendments, variations or adjustments, including deletions, additions & withdrawal or substitution as LabourDrive or its licensed provider deems fit.

1. Purpose and status

LabourDrive Proprietary Limited, registration number 2015/430580/07, (or its licensed provider) trading as LabourDrive, adopts this Policy to establish a practical governance framework for compliance with POPIA in its corporate operations and in the operation of the LabourDrive Platform ("the Platform").

The Policy is intended to support the eight conditions for lawful processing under POPIA, the duties of *responsible parties* and *operators*, and LabourDrive's (or its licensed provider's) contractual obligations to its Subscribers. It should be read with the Platform Privacy Policy, PAIA Manual, Platform Terms and Conditions, Data Processing & Privacy Schedule, related security policies and any incident-response procedures.

2. Scope

This Policy applies to directors, employees, contractors, developers, support personnel and other persons acting under LabourDrive's authority, and to personal information processed in corporate systems, the Platform, support systems, communications systems, integrations, backups and approved third-party services.

3. Governance roles

LabourDrive must maintain an Information Officer governance structure consistent with POPIA. The Information Officer remains accountable for statutory duties and may be assisted by duly designated and registered Deputy Information Officers.

For the present Policy, privacy correspondence should be directed to the CEO chris@labourdrive.com and the Deputy Information Officer contact is jason@labourdrive.com (+27 (0)79 877 2379).

LabourDrive acknowledges that operational responsibility for security, development, support, vendor management and legal compliance may be delegated internally, but statutory accountability is not avoided by such delegation.

4. Responsible party and operator framework

LabourDrive has identified its POPIA role in the table below for each material processing activity.

Processing context	Ordinary role	Governance consequence
Subscriber employee/ER data processed to provide Platform functionality on Subscriber instructions	LabourDrive: operator; Subscriber: responsible party	Process only with knowledge/authority; confidentiality; written contractual safeguards; incident notification to Subscriber.
Subscriber registration, billing, contract and support relationship	LabourDrive: responsible party	LabourDrive determines lawful purpose, notice, retention, security and data-subject response.
LabourDrive employees, contractors, directors and suppliers	LabourDrive: responsible party	Internal HR/supplier privacy controls apply.
Approved service provider processing LabourDrive-controlled data	Provider: operator to LabourDrive	Written operator terms and due diligence required.
Approved service provider processing Subscriber-controlled data through LabourDrive	Provider may a be sub-operator in the service chain – LabourDrive remains the operator; Subscriber: responsible party	Flow-down confidentiality/security obligations; processing limited to service-based purpose.

5. Lawfulness, minimality and purpose specification

Generally, it is acknowledged that personal information must be processed lawfully and in a reasonable manner that does not unjustifiably infringe privacy. Collection must be adequate, relevant and not excessive for the identified purpose. However, these general parameters are adjusted to cater for Platform related services – see Table in section 4 under: *Responsible party and operator framework*.

Before introducing a new material processing activity, feature or integration that relates to the Platform, LabourDrive will endeavour to identify: the information categories; data subjects; purpose; lawful basis; responsible-party/operator roles; recipients; location; retention; security risks; and whether special personal information, children's information, prior authorisation or cross-border restrictions are implicated.

6. Lawful bases and consent

It is necessary to acknowledge that consent on its own cannot be treated as the default legal basis for every employment-related data processing activity. LabourDrive therefore recognizes that the

appropriate POPIA basis must be identified in a given context, including consent, contractual necessity, legal obligation, protection of a legitimate interest, public-law duty where applicable, or legitimate interests. These criteria therefore apply relatively, based on the given context.

LabourDrive reasonably assumes that Platform subscribers are aware of the range of lawfulness provided for under POPIA's provisions. This approach seeks to embrace the available legal tenets enshrined within POPIA, thereby adopting a realistic and appropriate business approach towards Platform data processing.

Where consent is relied upon, it must be capable of being evidenced and withdrawal must be respected, subject to other lawful grounds that may continue to permit data processing. From a Platform Subscriber perspective, optional private-channel messaging should be separately managed from core employment records where appropriate or other suitable means.

7. Special personal information and children's information

LabourDrive acknowledges that special personal information must receive heightened control and should not be collected or uploaded merely because the Platform permits free-text or document uploads. Processing must be linked to a lawful ER purpose and a POPIA authorisation or applicable exception. However, LabourDrive reasonably assumes that Platform subscribers are aware of the range of lawfulness that apply to such aspects, provided for under POPIA's provisions.

8. Information quality

It is acknowledged that reasonable steps must be taken to ensure information is complete, accurate, not misleading and updated where necessary, having regard to the purpose. However, Subscribers of the Platform remain responsible for the substantive accuracy of Subscriber Content. LabourDrive is responsible for accuracy of corporate information it controls and for preserving Platform records without unauthorised alteration. The distinction between a *responsible party* and *operator* remains pertinent, as tabled in section 4 under: *Responsible party and operator framework*.

9. Openness and notices

LabourDrive will strive to maintain a clear Platform Privacy Policy and appropriate notices at relevant collection points. Where LabourDrive acts as operator, Subscribers remain responsible for their employee privacy notices, while LabourDrive provides contractual and product or service information thereby enabling Subscribers to explain the processing accurately.

10. Security safeguards programme

LabourDrive strives to maintain a documented, risk-based information-security programme appropriate to the sensitivity and volume of personal information and the nature of the Platform.

Security controls include some or all or a combination of the following criteria and may be reviewed periodically and after material changes or incidents.

- asset and data-flow identification for material systems;
- role-based access control, least privilege and timely de-provisioning;
- appropriate authentication controls and administrative-account protection;
- secure transmission and encryption controls appropriate to risk;
- logging, monitoring and auditability for security-relevant events;
- secure software development, change control, dependency and patch management;
- vulnerability management and periodic penetration testing or independent security assessment;
- backup, recovery, resilience and business-continuity controls;
- endpoint, network and cloud configuration controls appropriate to the architecture;
- staff confidentiality, awareness and incident-reporting obligations;
- vendor due diligence and written operator/sub-operator safeguards; and
- documented incident response, lessons learned and remediation tracking.

11. Access management

Access to personal information is granted on a need-to-know basis and reviewed periodically. Privileged access is tightly controlled and logged or overseen. Shared accounts are avoided where reasonably possible. Access must be revoked promptly when a person leaves or changes role.

Support or development access to Subscriber Content is limited to legitimate support, security, migration, integration or maintenance purposes and, where practicable, may use controlled support procedures rather than unrestricted standing access.

12. Operator and service-provider management

Before appointing a material operator or sub-operator, LabourDrive may conduct proportionate due diligence regarding security, privacy, service resilience, processing locations and contractual terms.

Written terms should require confidentiality and appropriate security measures and should address authorised purposes, incident notification, sub-processing, cross-border transfers, return/deletion, audit or assurance rights where appropriate, and cooperation with data-subject or regulatory requests.

13. Security compromise management

Any person acting for LabourDrive who becomes aware of suspected unauthorised access, acquisition, loss, disclosure or destruction of personal information must escalate it immediately under the incident-response procedure. This procedure is catered for in LabourDrive's PAIA Manual and may be complimented by additional operating procedures as LabourDrive sees fit.

Where LabourDrive is an operator for Subscriber-controlled information, LabourDrive shall notify the Subscriber promptly when there are reasonable grounds to believe unauthorised access or acquisition has occurred and provide information reasonably required for the Subscriber's POPIA response.

Where LabourDrive is the *responsible party*, the Information Officer shall ensure assessment, containment, preservation of evidence, mitigation and statutory notification to the Information Regulator and affected data subjects as required. A breach register and incident file should be maintained.

14. Data-subject requests

Requests for access, correction, deletion, destruction, objection or direct-marketing cessation must be routed to the Information Officer or Deputy Information Officer. Identity and authority must be verified proportionately.

Where LabourDrive is only an operator, the request should ordinarily be referred to the relevant Subscriber and LabourDrive shall reasonably assist. Where LabourDrive is the responsible party, the request is intended to be handled within the applicable POPIA/PAIA process and timeframes.

15. Retention and destruction

LabourDrive shall maintain a retention schedule covering corporate records and material Platform record classes. Retention must be tied to purpose, contract, statutory obligations, dispute/evidential needs and technical backup cycles.

Records that no longer need to be retained are aimed at being securely destroyed, deleted or de-identified. Destruction methods are aimed at being sufficient to prevent reconstruction in reasonably foreseeable circumstances. Backup deletion may occur through ordinary overwrite cycles provided access is restricted and the backup is not restored for unrelated purposes.

16. Cross-border transfers

Before transferring personal information to a third party in a foreign country, LabourDrive shall document the basis permitted by section 72 of POPIA, including adequate legal protection, binding corporate rules or agreement, consent where appropriate, contractual necessity or another applicable statutory basis.

Material cloud, AI, messaging and integration providers should be mapped by processing location and transfer mechanism.

17. AI, analytics and product development

AI features are generally designed to minimise unnecessary personal information, restrict use to authorised purposes and preserve human responsibility for employment and business decisions. Production Subscriber employee information shall not be repurposed for unrelated model training or product development unless a lawful basis, transparent notice and appropriate contractual authority exist.

Where analytics can reasonably be performed with aggregated or de-identified data, that approach should be preferred. Re-identification of de-identified Subscriber information is prohibited unless lawfully required for the original authorised purpose or otherwise contractually agreed.

18. Integrations and APIs

New integrations must undergo a data-flow and security review. Only the minimum required fields should be exchanged. Credentials, tokens and secrets must be protected and access scoped where the third-party API permits it.

Subscribers shall be informed of material data-sharing consequences before enabling optional integrations.

19. Training and confidentiality

Persons with access to personal information shall receive role-appropriate privacy and security awareness. Employment, contractor and service-provider arrangements should contain appropriate confidentiality obligations that survive termination where necessary.

20. Privacy impact and change review

A privacy and security review should be completed before materially changing processes involving high volumes of employee data, special personal information, systematic monitoring, new AI uses, new communications channels, new cross-border providers or significant integrations.

The review should record risks, mitigating controls, residual risk and accountable approval.

21. Direct marketing and cookies

Electronic direct marketing must comply with POPIA and other applicable laws, including consent/opt-out requirements. Operational service communications must be distinguished from marketing unless contractually specified with subscribers.

Website and Platform cookies or similar technologies must be inventoried and classified. Non-essential tracking should be subject to an appropriate lawful and transparent control mechanism.

22. Records of compliance

LabourDrive strives to maintain, as may be applicable: Information Officer registration evidence; PAIA Manual versions; PAIA annual reports; processing inventories; operator agreements; security assessments; breach register; data-subject request register; training records; retention schedule; vendor reviews; cross-border transfer records; privacy reviews; and policy approval/version history.

23. Review and enforcement

This Policy must be reviewed at least annually and after material legal, regulatory, security or Platform changes. Breaches by personnel or service providers may result in access restrictions, disciplinary or contractual action. Material compliance gaps or deficiencies must be escalated to senior management and the Information Officer.

All personnel and service providers of LabourDrive are urged to act cautiously, responsibly and with due diligence when dealing with and managing data privacy and related aspects.

Any reasonable suggestions and proposals for improving our approach towards data privacy, data protection and data management are welcome and should be forwarded to the Information Officer and/or Deputy Information Officer.

Please also refer to the LabourDrive Platform Privacy Policy and LabourDrive PAIA Manual.

Annexure A – Minimum General Processing Register Fields

Field	Minimum record
Activity	Name and business owner
Role	Responsible party / operator / sub-operator
Data subjects	Employees, users, subscribers, suppliers etc.
Information	Categories including special PI
Purpose	Specific and explicit purpose
Lawful basis	POPIA basis / authorisation
Recipients	Internal and third parties
Location	South Africa / foreign country
Retention	Period / trigger
Security	Key safeguards
Rights	Request-handling route
Review	Last / next review date