Cont@ct Labour (Pty) Ltd

LABOUR NEWS

ISSUE : MAY 2026 LEGAL EDITION!

POPIA in Practice: From Legal Foundations to Real-World Compliance

SOUND ADVICE & FAIR LABOUR PRACTICE

- HR Solutions
- Labour Relations
- Disciplinary Hearings
- CCMA Disputes
- Labour Law Practitioners
- EE & SDL Submissions

BROUGHT TO YOU BY CONTACT LABOUR (PTY) LTD

072 349 9596

admin@contactlabour.co.za

www.contactlabour.co.za

WHO MUST COMPLY?:

The Protection of Personal Information Act (POPIA) applies to every public and private body that processes personal information in South Africa. This legal mandate is not limited to large corporations; it includes businesses of all sizes, non-profits, and schools. If your organisation collects, stores, shares, or even destroys personal data —such as ID numbers, contact details, or financial history—you are legally required to be compliant.

THE CRITICAL DEADLINE:

While POPIA has governed South African data since 2021, your organisation faces a hard deadline on 30 June 2026 for pending submissions. With only weeks remaining, any entity - whether a business, school, or non-profit - that has not yet formalised its compliance framework is in a high-risk position.

THE CRITICAL DEADLINE:

Many organisations believe they are safe once they archive or discard data. However, under POPIA, the act of getting rid of data is still considered "processing". Simply putting records in a bin or archiving them without proper security is a violation; the law requires data to be shredded or digitally deleted in a way that it cannot be reconstructed.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

THE HIGH PRICE OF NON-COMPLIANCE:

Failing to adhere to POPIA carries severe legal and financial consequences designed to penalise negligence.

- **Massive Fines:** The Information Regulator has the authority to issue administrative fines of up to R10 million.
- **Imprisonment:** For serious criminal offences, including obstructing the Regulator or failing to comply with enforcement notices, individuals can face up to 10 years in prison.
- **Total Business Risk:** Beyond legal penalties, a single data breach can lead to irreparable reputational damage, loss of customer trust, and costly civil actions for damages.
- **Accountability:** You remain fully liable for ensuring compliance even if you outsource your data processing to a third party; the "Responsible Party" carries the risk for any violations committed by an operator.

THE SOLUTION:

Secure your compliance now. Navigating the complexities of a POPIA readiness assessment, appointing an Information Officer, and drafting mandatory PAIA manuals is a massive undertaking with zero room for error.

To protect your business from R10 million fines and criminal prosecution, professional guidance is essential. Reach out to Contact Labour today to get a quote and ensure your organisation is not the next example made by the Information Regulator.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

Cont@ct Labour
(Pty) Ltd

THE FOUNDATIONS OF DATA PRIVACY:

The Protection of Personal Information Act (POPIA), which came into full effect on 1 July 2021, is South Africa's primary law governing data privacy. It aims to protect the constitutional right to privacy by regulating how personal information is collected, stored, shared, and eventually destroyed. Every public and private body that processes personal information, including businesses of all sizes, non-profits, and schools, is legally required to comply. This legislation ensures that when organisations handle data, they do so in a manner that is lawful, fair, and transparent.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

UNDERSTANDING THE 8 CONDITIONS FOR LAWFUL PROCESSING:

POPIA sets out eight general conditions that serve as the "golden rules" for the lawful processing of personal information. These conditions must be met from the moment the purpose of processing is determined until the data is destroyed.

1. **Accountability:** The responsible party is fully liable for ensuring compliance, even if data processing is outsourced to a third party.
2. **Processing Limitation:** Personal information must be processed lawfully and only if it is adequate, relevant, and not excessive for its intended purpose.
3. **Purpose Specification:** Data must be collected for a specific, explicitly defined, and lawful purpose related to the organisation's functions.
4. **Further Processing Limitation:** Any subsequent use of information must be compatible with the original purpose for which it was collected.
5. **Information Quality:** Organisations must take reasonable steps to ensure that personal information is complete, accurate, and kept up to date.
6. **Openness:** Data subjects must be informed about what information is being collected, who is collecting it, and why.
7. **Security Safeguards:** Organisations must implement appropriate technical and organisational measures to prevent data loss, damage, or unauthorised access.
8. **Data Subject Participation:** Individuals have the right to access their information and request the correction or deletion of inaccurate or unlawfully obtained data.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

ORDINARY VS. SPECIAL PERSONAL INFORMATION:

POPIA DISTINGUISHES BETWEEN TWO MAIN CATEGORIES OF DATA, WITH THE LATTER REQUIRING SIGNIFICANTLY MORE PROTECTION:

Ordinary Personal Information:
This includes data such as identity numbers, addresses, contact details, employment history, financial data, and opinions.

Special Personal Information:
This refers to sensitive data that is generally prohibited from being processed unless a specific exemption or consent applies.

IT INCLUDES:

- Religious or philosophical beliefs.
- Race or ethnic origin.
- Trade union membership.
- Political persuasion.
- Health, sex life, or sexual orientation.
- Criminal behaviour or alleged offences
- Biometric information (e.g., fingerprints, DNA, or blood type).

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

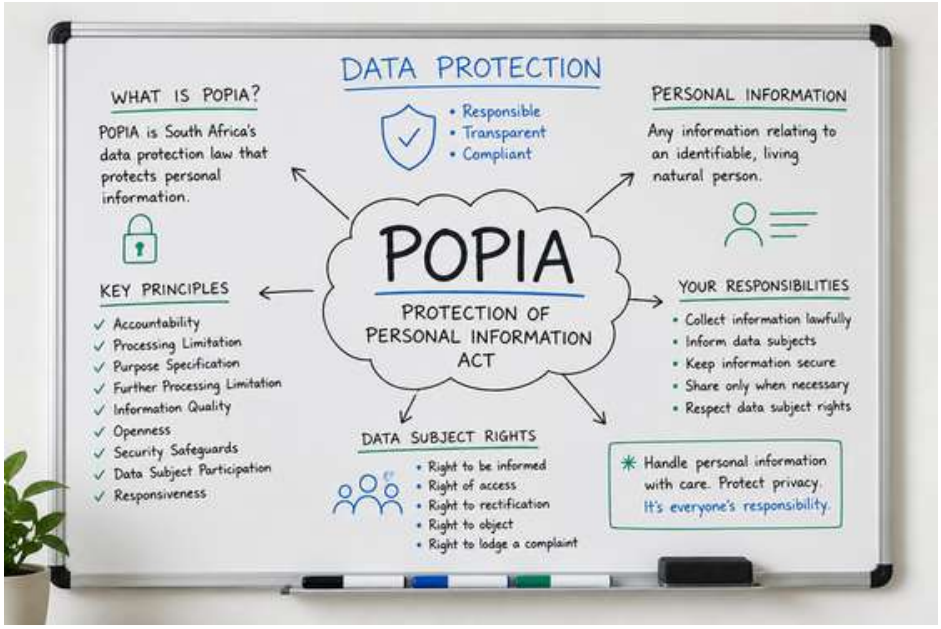
PROCESSING CHILDREN'S INFORMATION:

THE ACT PROVIDES STRICT PROTECTIONS FOR CHILDREN (NATURAL PERSONS UNDER 18 WHO ARE NOT LEGALLY COMPETENT).

General Prohibition:
Processing a child's personal information is prohibited.

The Competent Person:
To lawfully process a child's data, you must typically obtain the prior consent of a competent person, such as a parent or legal guardian.

Exceptions:
Processing is allowed without consent only if it is necessary for a legal obligation, a right in law, or if the information has been deliberately made public by the child with the consent of a competent person.



T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

WHEN PRIOR AUTHORISATION IS MANDATORY:

CERTAIN HIGH-RISK PROCESSING ACTIVITIES REQUIRE YOU TO OBTAIN APPROVAL FROM THE INFORMATION REGULATOR BEFORE YOU BEGIN.

PRIOR AUTHORISATION IS NEEDED IF YOU PLAN TO:

Link Unique Identifiers:
Link information (like ID numbers) across different responsible parties for a purpose other than the original collection intent.

Process Criminal Records:
Handle information regarding criminal behaviour or unlawful conduct on behalf of third parties.

Credit Reporting:
Process information for the purposes of credit reporting.

High-Risk Transborder Transfers:
Transfer special personal information or children's information to a third party in a foreign country that does not provide adequate data protection.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

MANAGING OPERATORS (THIRD-PARTY SERVICE PROVIDERS)

MANY ORGANISATIONS OUTSOURCE FUNCTIONS LIKE PAYROLL OR IT SUPPORT TO "OPERATORS".

Accountability remains with you:
The "Responsible Party" (your organisation) is legally liable for any POPIA violations committed by an Operator, even if the mistake was theirs.

Written Contracts:
You must have a written contract with every Operator. This contract must mandate that the Operator implements technical and organisational security measures and treats the data as confidential.

Breach Notification:
Operators are legally required to notify the Responsible Party immediately if they suspect a data breach

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

PRACTICAL STEPS:
THE COMPLIANCE CHECKLIST:

A STRUCTURED APPROACH TO IMPLEMENTING POPIA:

Step 1: *Mobilise a Team:*
Appoint an Information Officer, register them with the Regulator and create a project plan with priorities.

Step 2: *Readiness Assessment:*
Conduct a gap analysis to identify where your current data handling practices fail to meet POPIA standards.

Step 3: *Core Documentation:*
Develop a PAIA Manual (required by law), a Privacy Policy, and an Incident Management Policy.

Step 4: *Update Procedures:*
Review Standard Operating Procedures (SOPs) for the entire data lifecycle, from collection to destruction.

Step 5: *Training:*
Conduct regular awareness sessions for all staff to ensure they understand their specific responsibilities in protecting data.

Step 6: *Disposal:*
Establish a process to permanently delete or shred information once it is no longer needed, ensuring it cannot be reconstructed.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

Cont@ct Labour
(Pty) Ltd.

SPOTLIGHT ON THE INFORMATION OFFICER:

The Information Officer (IO) is a pivotal figure responsible for overseeing an organisation's POPIA compliance. Under the Act, the head of the business -such as the CEO or sole trader - is automatically designated as the IO. The IO's duties include developing a compliance framework, conducting personal information impact assessments, and liaising with the Information Regulator. It is a mandatory requirement that the IO and any Deputy Information Officers register with the Information Regulator before they can legally commence their duties.

DATA BREACH READINESS AND SECURITY MEASURES:

A data breach occurs whenever personal information is accessed or acquired by an unauthorised person. To mitigate this risk, organisations must establish robust security safeguards, such as firewalls, encryption, and secure backups, while also maintaining physical security like locked filing cabinets. If a security compromise is suspected, the responsible party is legally mandated to notify the Information Regulator and the affected data subjects as soon as reasonably possible. This written notification must provide enough detail for data subjects to take protective measures against potential consequences.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

THE HIGH PRICE OF NON-COMPLIANCE:

Failing to adhere to POPIA can result in severe legal and financial repercussions. The Information Regulator has the power to issue administrative fines of up to R10 million. For serious criminal offenses, such as obstructing the Regulator or failing to comply with enforcement notices, individuals may face imprisonment for up to 10 years. Beyond these penalties, organisations risk significant reputational damage, loss of customer trust and civil actions for damages.

BUILDING A CULTURE OF COMPLIANCE:

Achieving compliance is an ongoing journey rather than a one-off project. Organisations should start by conducting a POPIA readiness assessment to identify gaps in their current practices. Key actions include drafting a clear Privacy Policy, maintaining an updated PAIA Manual, and ensuring that all third-party contracts contain POPIA-compliant clauses. Finally, regular internal awareness and training sessions for all staff members are crucial for embedding a culture where protecting personal information becomes "business as usual"

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

FINAL THOUGHT:

POPIA compliance is not merely a legal checkbox but a fundamental shift toward embedding data protection into the very fabric of an organisation's operations. It requires a culture where safeguarding personal information is recognised as a fundamental human right and an ongoing "business as usual" responsibility. Just as a ship requires a sturdy hull, a vigilant lookout and a well-practiced emergency plan to navigate safely, an organisation needs a robust compliance framework and constant vigilance to protect the valuable cargo of personal information entrusted to its care.

INTERESTING FACT:

Most people associate "processing" with active use or sharing, but under POPIA, an organisation is still legally processing data even as they are getting rid of it.
Because this final act is considered processing, the law requires that it must be done in a secure manner that permanently prevents the information from being reconstructed in an intelligible form.
Simply archiving records or putting them in a bin is not enough; they must be shredded or digitally deleted so they are gone for good.

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za

12-MONTH COMPREHENSIVE POPI COMPLIANCE PROGRAMME

Month 1:

Appoint & Register

Month 2:

- Deep data mapping
- Operators register
- Data-flow diagrams

Month 3 - 4:

- Policy development & approvals (incl. POPI Management, Risk Policy, Cookie/Website privacy, Marketing governance)

Month 5:

- Multi-audience training
- Responsibilities matrix

Month 6-7:

- Implementation sprints
- DSAR portal/form
- Breach drill
- Evidence pack

Month 8:

- Internal assessment
- Final Compliance Report
- Annual refresh calendar

Add-ons:

- Submission, Website cookie banner + privacy center
- Breach simulation
- Quarterly health-checks
- Cross-border transfer assessments

Our Tailored Program Ensures Your Business Meets All Compliance Requirements While Integrating Cultural Practices Seamlessly. With A Structured Approach, We Guide You Through Each Step Of The Process.

Cultural Integration & Full Audit Defense

(R2493.75 Per Month)

CONNECT WITH US

Want guidance on drafting compliant contracts? Need help avoiding Labour disputes?

Let's talk!
Email address: admin@contactlabour.co.za
Contact number: 072 349 9596

📱 Follow us on social for tips, updates & case studies:

HERE ARE THE LINKS:

https://www.linkedin.com/company/contact-labour/?viewAsMember=true

Our Strategic Partnership

T) 072 349 9596
admin@contactlabour.co.za
www.contactlabour.co.za