Cont@ct Labour
(Pty) Ltd.

LABOUR NEWS

ISSUE: OCTOBER 2025

POPI – COMPLIANCE CRUNCH

SOUND ADVICE & FAIR LABOUR PRACTICE

072 349 9596 (T)

admin@contactlabour.co.za

www.contactlabour.co.za

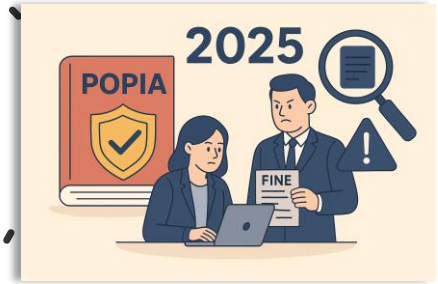
Cont@ct Labour (Pty) Ltd.

Welcome to the Age of the Demonstrable Safeguard.

Once upon a time, organisations believed the Protection of Personal Information Act, 2013 (POPIA), was a regulatory hurdle set far in the future. The grace period for full compliance ended on 1 July 2021, yet for the few years following, some employers may have remained complacent or disregarded the new legal requirements.

Fast forward to 2025: The Information Regulator has significantly escalated its monitoring and enforcement activities, turning up the pressure to achieve universal adherence. It's now definitively the era of mandatory compliance, building on the precedent set by the first administrative fine issued in July 2023.

For organisations, this means ensuring compliance is truly "business as usual". For the Regulator, it means actively issuing infringement notices and imposing administrative fines of up to R10 million for violations, particularly against those who fail to remedy security shortcomings or ignore an enforcement notice. The Regulator has signalled that there will be more penalties and administrative fines issued for POPIA violations.



The Regulator now also has the authority to conduct investigations, issue compliance directives, and refer matters for criminal prosecution where necessary. In certain cases, directors or officers of an organisation may be held personally liable.

QUESTION: What does the term 'processing' mean under POPIA?

ANSWER: Any operation or activity concerning personal information, including its collection, storage, use, dissemination, or destruction.

T) 072 349 9596 (F) 086 519 7505
admin@contactlabour.co.za
www.contactlabour.co.za

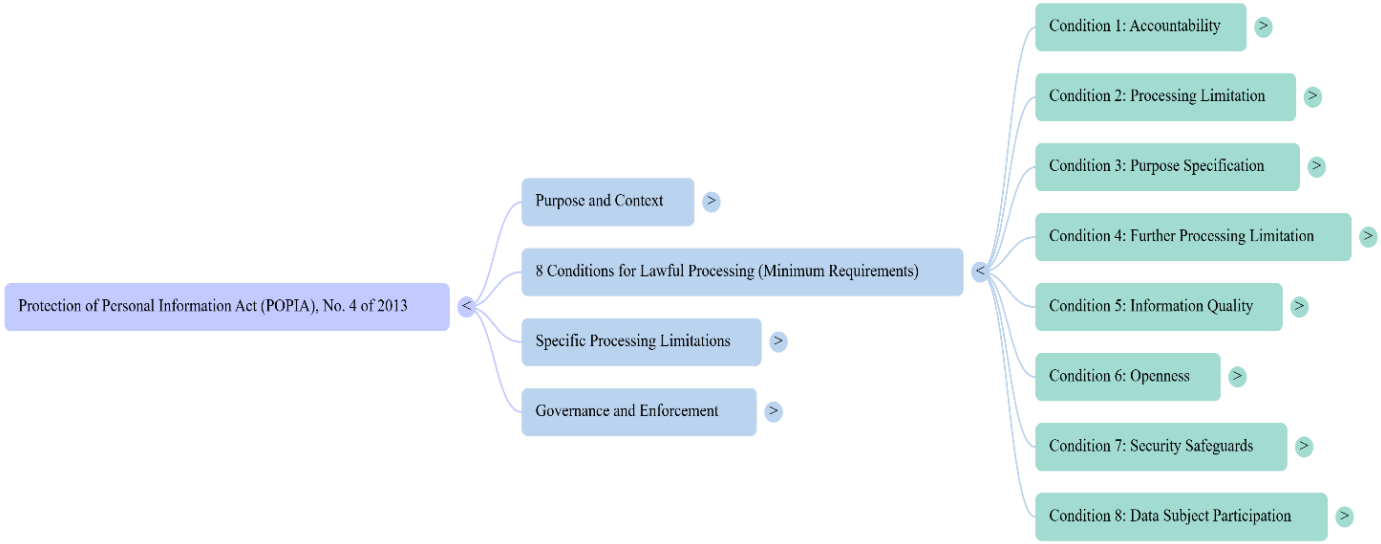
Don't Ignore Enforcement: The Consequences of Non-Compliance

The core challenge for every Responsible Party is demonstrating continuous compliance with the Eight Conditions for Lawful Processing. If handled negligently, non-compliance can result in severe financial and reputational losses.

The employer's job is to ensure robust security and timely action and act immediately when a breach or notice occurs.

Immediate Steps to Protect Your Organisation

To mitigate risk and ensure POPIA compliance remains a fundamental part of your operations, ensure the following core elements are continuously in place:



Analogy: Imagine these eight conditions as the **eight essential safety checks for a ship carrying valuable cargo (personal information)**.

1. **Accountability** is like the captain's ultimate responsibility: even if the crew (operators) handles the cargo, the captain is accountable for its safe passage.
2. **Processing Limitation** means only loading necessary cargo, handled carefully, and only with the owner's permission or a clear reason.
3. **Purpose Specification** is knowing exactly where the cargo is going and why, and making sure it's delivered and not kept indefinitely.
4. **Further Processing Limitation** ensures that once the cargo reaches its destination, it's not diverted for an entirely different, unapproved journey.
5. **Information Quality** is making sure the cargo manifests are accurate and up-to-date, so you know exactly what's on board.
6. **Openness** means clearly communicating to the cargo owners where their goods are, what's being done with them, and who's responsible.
7. **Security Safeguards** are the locks, guards, and secure containers protecting the cargo from theft or damage, continuously updated against new piracy threats.
8. **Data Subject Participation** gives the cargo owners the right to check their manifest, correct errors, and request the removal of their goods if the journey is no longer justified.

Failing any of these checks could put the valuable cargo at risk and lead to severe consequences for the ship and its crew.

- **Appoint and register the IO:** The head of the business is automatically the Information Officer (IO) but may delegate this role to a senior person; however, accountability cannot be contracted out. The IO and any designated Deputy Information Officers (DIOs) must be registered with the Information Regulator before commencing their duties. The IO should also establish a compliance framework, monitor its effectiveness and report directly to the Regulator when required.
- **Maintain Compliance Documentation:** The IO must develop, maintain and make available a POPI / PAIA manual that details processing purposes, data subject categories, recipients, planned transborder flows and a general description of security measures. This documentation serves as both an internal guide and external assurance to stakeholders, making transparency and accountability demonstrable.

- **Manage Data Subject Rights:** Ensure accessible processes are established to manage the rights of data subjects, including the right to inquire whether personal information is held, the right to request access (which may incur a prescribed fee for copies) and the right to request correction or deletion of inaccurate or unlawfully retained PI. Data subjects may use Form 2 for requests for correction or deletion. These processes must be simple, accessible, and well-communicated to employees, clients and the public. Organisations must also ensure that requests are responded to within the legally prescribed timelines.

- **Review Operator Contracts:** If you outsource PI processing, ensure there is a written contract with the Operator stipulating that they maintain adequate security measures. The contract must require the Operator to implement safeguards, act only under your documented instructions, and notify you immediately in the event of a data breach. Contracts should be reviewed regularly to align with evolving risks and regulatory updates.
- **Implement Retention & Destruction Policies:** Organisations must not retain personal information longer than necessary for the purpose it was collected, unless a longer retention period is legally required. Clear retention schedules and secure destruction methods (e.g., shredding, secure digital wiping) must be in place.
- **Train Employees on POPIA Responsibilities:** Employees are often the first point of contact with personal information. Ongoing training ensures they understand how to handle PI responsibly, identify potential breaches, and follow correct escalation protocols.
- **Conduct Regular Compliance Audits:** Schedule periodic audits to assess current practices against POPIA requirements. Document corrective actions, update risk registers, and provide reports to leadership to ensure accountability.

POPI COMPLIANCE CHECKLIST: ESSENTIAL PILLARS

Key Focus Areas for Ongoing Compliance:

1. **Security Safeguards (Condition 7): Protect your Data Fortress**

   Responsible parties must secure the integrity and confidentiality of personal information (PI) by taking appropriate, reasonable technical and organisational measures to prevent loss, damage, or unlawful access. This includes identifying risks, establishing and maintaining appropriate safeguards, regularly verifying their effectiveness, and continuously updating them in

response to new risks. Examples of safeguards include encryption, access control systems, staff training, secure storage and regular penetration testing to identify vulnerabilities.

2. **Breach Notification (Section 22): Act Fast, Notify Right**

If a security compromise occurs and PI is accessed by an unauthorised person, the Responsible Party must notify both the Information Regulator and the affected data subjects. This notification must occur as soon as reasonably possible after the discovery of the compromise. The notification must be in writing and provide sufficient information for data subjects to take protective measures. Organisations should have a documented incident response plan, including internal reporting lines, timelines and template notification letters, to ensure compliance with this obligation.

3. **Complying with Enforcement Notices: The Final Warning**

If the Regulator finds shortcomings, they may issue an Enforcement Notice (Form 15). This notice specifies corrective actions to be taken, or processing to be stopped, within a defined period. Failure to comply with an enforcement notice is deemed a serious offence. Organisations should prepare by keeping a compliance evidence trail, conducting regular audits, and ensuring their Information Officer can respond swiftly with corrective actions.

The Information Regulator issued its **first administrative fine of R5 million** in July 2023. This sanction was issued against the Department of Justice and Constitutional Development (DoJ&CD) for **failing to comply with an enforcement notice** after previous data breaches. This included a failure to renew critical security software licenses.

Cont@ct Labour (Pty) Ltd.

Grab the POPI Compliance Questionnaire, fill it in, and send to jade@contactlabour.co.za. We'll check your POPI compliance and get back to you. **Download here -> POPI COMPLIANCY QUESTIONNAIRE**

Sincerely yours!

Jade Viviers and Novana Pillay

Do you know about our new Facebook and LinkedIn Business pages we just launched for Contact Labour. This is where we will be sharing our best tips to help with any Labour Relations problems or queries you might have. We would really appreciate it if you like our new pages and if you do, you will get our best content first.

Here are the links:

https://www.facebook.com/contactlabour

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

T) 072 349 9596 (F) 086 519 7505
admin@contactlabour.co.za
www.contactlabour.co.za

Cont@ct Labour (Pty) Ltd.

ENDORSEMENT FOR UITKYK SKRYFBEHOEFTES

At **Contact Labour**, we are proud to endorse **Uitkyk Stationery** as our trusted supplier for all office essentials. Their commitment to **quality products**, **competitive pricing**, **and exceptional customer service** ensures that we can keep our workplace running smoothly.

We especially value their **"Stationery in a Flash"** service – offering same-day delivery within 90 minutes for qualifying orders. This efficiency saves us valuable time and guarantees that our teams are always equipped with the tools they need. Uitkyk Stationery is more than just a supplier – they are a **reliable partner** in supporting our productivity and success.