The Protection of Personal Information Act

From an employment perspective

Jacques van Wyk, director: labour and employment law
at Werksmans Attorneys
Jacques van Wyk is the director: labour and employment law at Werksmans Attorneys. He has a BA (LLB) from the University of Cape Town. He practises labour and employment law, as well as business crime and forensics law. Jacques was named as a recommended lawyer in labour & employment by the Legal500 (2010 - 2012) and he co-authored *Labour Law in Action – A Handbook on the new Labour Relations Act 1997*– with Frances Anderson.
Contents

2  How can you process information legally? ................................................................. 4
2.1 Condition 1: accountability .................................................................................. 4
2.2 Condition 2: limitations on processing ................................................................. 5
2.3 Condition 3: purpose specification ...................................................................... 5
2.4 Condition 4: further processing limitation ........................................................... 6
2.5 Condition 5: information quality .......................................................................... 6
2.6 Condition 6: openness .......................................................................................... 6
2.7 Condition 7: security safeguards ......................................................................... 7
2.8 Condition 8: employee participation .................................................................... 7
3.  Processing of ‘special personal information’ .......................................................... 7
4.  Automated decision-making .................................................................................... 8
5.  Trans-border information flows .............................................................................. 9
6.  Conclusion: how to ensure you’re POPI compliant ............................................... 9
The Protection of Personal Information (POPI) Act No. 4 of 2003 – assented to in November 2013 - places significant obligations on most individuals and juristic entities. Most importantly, this act put substantial duties on employers.

POPI’s purpose is to give effect to the constitutional right to privacy by introducing measures to ensure data subjects’ personal information, i.e. employees, is safeguarded when responsible parties, i.e. employers, process it.

Employers will have to comply with the principles enshrined in POPI whenever their employees’ personal information is collected, stored or used:

- If the employer breaches the duties imposed by POPI, it could be faced with an administrative fine of up to R10 000 000.

Owing to the serious consequences that arise from non-compliance with this act, it’s essential employers rigidly stick to POPI’s provisions by putting compliance procedures in place to ensure the obligations imposed on them are satisfied.

Most information employers collect from employees will be considered ‘personal information’, e.g.:

- Information about an employee’s:
  - Race,
  - Age,
  - Gender,
  - Sex,
  - Pregnancy status,
  - Marital status,
  - Nationality,
  - Ethnic or social origin,
  - Sexual orientation,
  - Physical or mental health,
  - Disability status,
  - Religion, and
  - Culture and language.

- Information relating to employees’:
  - Educational,
  - Medical,
  - Financial,
  - Criminal, or
Employment history.

- Information related to the employees’ location, e.g.:
  - E-Mail and physical addresses, and
  - Telephone and cellphone numbers.

- Employees’ biometric information – e.g. fingerprints and retinal data – gathered from fingerprint and retina scanners.

- Correspondence that the employee sends which is, implicitly or explicitly, of a private or confidential nature, e.g. a personal e-mail.

**Personal information must be processed lawfully**

‘Processing’ is broadly defined as being any operation or activity - whether or not by automatic means - that concerns personal information. This includes:

- Collection,
- Recording,
- Organisation,
- Collation,
- Storage,
- Updating or modification,
- Transmission,
- Distribution,
- Making it available in any other form,
- Linking,
- Restriction,
- Degradation,
- Erasure,
- Destruction,
- Retrieval, and
- Consultation or use of information.

**2 How can you process information legally?**

**2.1 Condition 1: accountability**

The employer must ensure that he complies with the eight conditions set out in POPI. He must comply with these conditions when the purpose and method of processing has been determined as well as during the processing itself.

Employers must appoint an information officer and deputy information officers to ensure they comply with these conditions and deal with complaints from employees who want to enforce POPI. These individuals may be appointed from your current staff members.
2.2 Condition 2: limitations on processing

POPI imposes several limitations on how an employer may process an employee’s personal information:

- The processing must be lawful:
  - It may not be against South African law, and
  - It must be conducted in a reasonable manner that doesn’t infringe on the employee’s privacy.\(^1\)
  - It must be necessary in order for a public body to perform a public law duty properly.

- The personal information an employer processes must also be adequate, relevant, not excessive and relate to why the processing was undertaken.

- An employer may only process his employees’ personal information if there’s a good reason why this processing needs to take place, e.g. where the:
  - Employee gave fully informed and proper consent to the processing,\(^2\)
  - Processing is necessary to conclude or perform the employment contract, or
  - Employer is legally obliged to carry out the processing.\(^3\)

- The processing must protect the employee’s legitimate interest.\(^4\)

- Personal information must be obtained directly from the employee unless:
  - The employer has received his employee’s consent to do otherwise, or
  - Where the information has been made publically available, e.g. on social media platforms such as Facebook.

2.3 Condition 3: purpose specification

When the employer collects personal information, it may only do so for specific, explicitly defined and lawful purposes related to its function. Steps must be taken to ensure that employees are made aware of this purpose.

---

\(^1\) Terms such as ‘reasonable manner’ and ‘privacy’ are not defined in POPI. Case law will have to be consulted to deal with the constitutional right to privacy to give meaning to these terms.

\(^2\) The employer bears the onus to prove that such consent was provided and the employee may withdraw consent at any time.

\(^3\) An example would be the obligation for an employer to store employee information in accordance with the provisions of the Basic Conditions of Employment Act 75 of 1997, as amended (BCEA), and the Labour Relations Act 66 of 1995, as amended (LRA).

\(^4\) The term ‘legitimate interest’ isn’t defined in POPI. Given the wide connotations of the term, this introduces an element of uncertainty, the boundaries of which will only be demarcated in practice. However, a likely example of such an interest will be the employee’s medical history and needs. Equally undefined is the justification that processing is necessary for pursuing the legitimate interests of the employer, or of a third party to whom the information is supplied. The latter justification leaves a large discretion to the employer to determine its legitimate interests.
Employers may only keep personal information for as long as a law or code of conduct, determined by the information regulator, provides:

- In the absence of a law or code of conduct, the retention period must be long enough to afford the employee a reasonable opportunity to request access to the records.
- An employer may not keep any personal information records for longer than is necessary to achieve the purpose the information was collected for. An exception to this limitation would be where the employment contract requires the records to be kept longer. This allows for the employer to regulate the obligations bestowed on it through using its employment contracts.

2.4 Condition 4: further processing limitation
If an employer wishes to process information more than once, the subsequent processing must also:

- Comply with the conditions set out in POPI, and
- Be compatible with the original purposes for which the information was collected.

An example would be where the employer collects the e-mail addresses of each of his employees and then makes this list available to all staff members by e-mailing it to each employee. Making the list available would be ‘processing’ and would have to comply with why the e-mail addresses were collected in the first place.

2.5 Condition 5: information quality
An employer must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary. The employer must keep the purpose, for which personal information was collected or is further processed further, in mind.

2.6 Condition 6: openness
An employer must maintain documentation for all processing. A particularly onerous duty placed on the employer is that before processing, it must take reasonably practicable steps to ensure that the employee is aware of a number of facts, such as:

- What information is being collected,
- The purpose of such collection, and
- Who will have access to the information.

If the employer intends to transfer the information to a country outside South Africa, the employee must be notified of this.

The employee must also be informed of his or her right to access the information and the right to rectify it as well as the right to object to the processing of personal information. Similarly, an employee must be informed of his right to lodge a complaint with the information regulator and the contact details thereof.
NB: It’s recommended that all the information above be incorporated into the employment contract to cater for information that the employer knows or predicts will be processed.

2.7 Condition 7: security safeguards

An employer must secure the integrity and confidentiality of personal information in its possession or under its control. This must be achieved by taking appropriate and reasonable technical and organisational measures to prevent:

- Loss,
- Damage, or
- The unlawful access or processing of personal information.

The employer must:

- Take practical measures to identify all reasonably foreseeable internal and external security risks and establish appropriate safeguards,
- Have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of a specific industry or professional rules and regulations, and
- Ensure they have updated antivirus software and firewalls to protect digitally stored personal information.

Where there are reasonable grounds to believe that an employee’s personal information has been accessed or acquired by any unauthorised person, the employer must notify the information regulator and the employee as soon as possible.

2.8 Condition 8: employee participation

An employee has the right to request access to his personal information records, which his employer holds. The record must be provided within a reasonable time, manner and form, and possibly at a prescribed fee. The employee has a right to request that the record be corrected or deleted if this is warranted.

If an employer receives such a request but refuses to comply, it must provide the employee with a notification to that effect. It must also attach a note to the record that a particular request was made but was not executed.

3. Processing of ‘special personal information’

‘Special personal information’ means an employee’s personal information that relates to the:

- Religion,

---

5 Ideally, backups should be made on a remote server to be prepared for accidental deletion or local hard drive failure. Regular IT maintenance is also recommended. Physical records must only be accessible by authorised personnel and should be kept in a secure location.
• Race or ethnic origin,
• Trade union membership,
• Political persuasion,
• Health,
• Sex life,
• Biometric information or
• Criminal behaviour.

Employers may not process such information unless:
• They are given general authorisation\textsuperscript{6}, or
• If a listed exception applies for specific categories of special personal information,
• The employee posts the information on Facebook,
• The information regulator has authorised such processing after application by the employer or where processing is for statistical purposes, and

If the employee is only identified when it’s essential for the required purpose and to comply with affirmative action laws and measures such as BEE legislation, an employer may process information concerning an employee’s race or ethnic origin.

The prohibition on processing personal information concerning an employee’s trade union membership doesn’t apply to the trade union the employee belongs to if this processing is necessary to achieve the union’s aims.

No information regarding trade union membership may be supplied by trade unions to third parties without consent from the employee:
• When employers want to provide employees with the benefits or rights obtained through collective bargaining, the general authorisation referred to above would be applied.

4. Automated decision-making

An employee may not be subject to a decision resulting in legal consequences for - or affecting - him to substantial degree. This decision is based solely on automated processing.

Examples of automated decision-making would be:
• Processing personal information, and
• Using software to create a profile of the employee, including his:
  – Performance at work,

\textsuperscript{6} ‘General authorisation’ would be granted in cases where the employee consents to the processing and where processing is necessary to establish, exercise or defend a right or obligation in law or where the employee deliberately makes the information publically available.
− Credit worthiness,
− Reliability,
− Location,
− Health,
− Personal preferences, or
− Conduct.

An exception to the principle outlined above would be where the automated decision has been taken in terms of the employment contract or is authorised by a law or code of conduct. As long as appropriate measures are taken to protect the employee’s legitimate interests, the automated decision-making will be lawful.

5. Trans-border information flows

POPI also contains provisions relating to the distribution of information by a South African entity to a third party in a foreign country. This is particularly relevant to groups of companies with both South African and foreign branches or subsidiaries.

An employer may not transfer personal information about an employee to a third party who’s in a foreign country unless the third party is subject to a law or agreement that provides substantially similar principles for reasonable processing, as contained in POPI.

This provision is especially onerous as employers would have to perform research to ascertain this information. The same applies to the further transfer of personal information from one third party to other third parties in foreign countries.

6. Conclusion: how to ensure you’re POPI compliant

In light of the duties imposed on employers, it’s recommended that you, the employer, take the following steps to ensure compliance with POPI:

• Ensure your staff - especially those who process employee information on a regular basis, e.g. HR and IT officials – know what duties POPI imposes on employers.

• Appoint an information officer and deputy information officers.

• Draw up a data privacy policy and make all your employees familiar with its contents. The policy should include protocols that enable employees to lodge complaints against processing.

• Implement a document-retention policy to ensure employees’ personal information records are destroyed in reasonable periods.

• Word employment contracts broadly when you need the employee to consent to processing so you can cater for the broad definition of ‘processing’ in POPI. Ensure that these contracts incorporate sufficient information that is relevant to the processing so that it can be said an employee gave informed consent.
• Take care when you process ‘special personal information’ such as ethnicity and trade union membership. Ensure proper security safeguards are in place to protect personal information from unauthorised access or deletion.

• Comply with POPI regarding how you transfer personal information to third parties in foreign countries. Perform legal research to determine if the country, to which the information is being transferred, has promulgated privacy protection legislation similar to POPI.