THE PROTECTION OF PERSONAL INFORMATION ACT, NO 4 OF 2013
THE PROTECTION OF PERSONAL INFORMATION ACT, NO 4 OF 2013

APPLICATION IN THE WORKPLACE

Has the Protection of Personal Information Act, NO 4 of 2013 (POPI) commenced?

Only certain sections have commenced. The sections relate to the definitions, the Information Regulator, the regulations and procedures for making regulations.

In December 2018, the Information Regulator published regulations (2018 Regulations), however the commencement date of the 2018 Regulations is yet to be determined.

The remaining sections of POPI are intended to come into operation once the Information Regulator is fully operational. Compliance with POPI’s obligations relating to the processing of information will then still be suspended for at least one year, to allow responsible parties to achieve compliance with POPI.
What is the purpose of POPI?

The preamble to POPI records that POPI emanates from s14 of the Constitution of the Republic of South Africa, 1996, which section provides that everyone has the right to privacy and it includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

POPI gives expression to the constitutional values of democracy and openness, recognising the need for economic and social progress within the framework of the information society and the need for a removal of unnecessary impediments to the free flow of information, including personal information.

POPI has been promulgated to regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests.

Does POPI apply to employers and their employees?

POPI hails a new dispensation for employers and employees. It introduces obligations on employers and grants rights to employees in an attempt to balance the right of employers to conduct a business with the right to the privacy of its employees. POPI is not limited to the parties to an employment relationship, but there is no doubt that they are subject to its protections.

WHAT EMPLOYMENT RELATED INFORMATION IS PROTECTED IN TERMS OF POPI?

What information is covered?

POPI covers all information that employers might collect, retain or archive on any individual who might wish to work, work, or have worked for the employer. This includes both personal and special personal information.

What is ‘personal information’?

Personal information is information which is about a living identifiable person (a ‘data subject’) and affects that person’s privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature and identifies a person, whether by itself, or together with other information in the organisation’s possession or that is likely to come into its possession.

Personal information likely to be covered by POPI may include details of an employee’s salary and bank account, e-mails about an incident, a supervisor’s notebook, an individual employee’s personnel file, leave records, performance reviews, a set of leave cards depending upon how they are kept and a set of completed application forms filed in a particular order.

What is ‘special personal information’?

Special personal information is information concerning an individual’s religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, the criminal behaviour of a person subject to the extent that such information relates to the alleged commission by the employee of any offence or any proceedings in respect of any offence allegedly committed by an employee or about the disposal of such proceedings.

‘Data subjects’: who are they within an employment context?

POPI refers to the persons to whom personal information relates, as ‘data subjects’. Within an employment context, this includes applicants and former applicants (successful or unsuccessful), former or current employees, Temporary Employment Services staff, casual staff, staff on secondment and those on work experience placements. The personal information of all of these people must be dealt with in accordance with POPI.

What manifestations of information are covered by POPI?

POPI applies to any personal information entered into any record by an employer. A record includes any writing on any material, labels, books, maps, plans, graphs, drawings and photographs, films, negatives, tapes or other devices where visual images are stored.

Personal information about individuals that is kept by an employer on a computerised system in the employment context will fall within the scope of the POPI subject to some exceptions.
WHAT DOES ‘PROCESSING’ OR ‘FURTHER PROCESSING’ OF INFORMATION MEAN?

POPI applies only to personal information and special personal information that is subject to ‘processing’ or ‘further processing’. The term ‘processing’ applies to a comprehensive range of activities. It includes the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal of the data. The processing of personal information in the workplace from recruitment to retirement is covered. Likely activities that will constitute processing or further processing of personal or special personal information are:

- The recruitment and selection process commencing with the advertising of vacancies, receiving, sorting and storing of applications, the shortlisting process, interviews, vetting and verifying of data provided by the applicant (data subject), communications to successful and unsuccessful applicants and letters of appointment
- Processing payment of remuneration, recording bank account details, payslips and tax records
- Receiving and storing of leave applications and records, sick leave and medical records, records and communications relating to injuries on duty and otherwise
- Monitoring performance, conducting written performance assessments, dealing with promotions and demotions and the records of disciplinary processes
- Obtaining distributing and storing information relating to medical aid membership, medical aid claims, payment of medical aid subscriptions, membership of retirement funds, contributions to retirement funds and their administrators and retirement benefits
- Obtaining, creating and storing of information relating to termination of employment, the issue of references and exit interviews
- The exchange of information of staff members in a business transfer or out sourcing transaction

WHEN WILL IT BE LAWFUL TO PROCESS INFORMATION?

Processing and further processing of personal information is only lawful if it complies with the eight conditions specified in POPI. An employee (data subject) has the right to have his or her personal information processed in accordance with these conditions. The eight conditions for the lawful processing of personal information are:

- Accountability, as referred to in s8
- Processing limitation, as referred to in s9 to 12
- Purpose specification, as referred to in s13 and 14
- Further processing limitation, as referred to in s15
- Information quality, as referred to in s16
- Openness, as referred to in s17 and 18
- Security safeguards, as referred to in s19 to 22
- Data subject participation, as referred to in s23 to 25

An employee in addition has the right to access to his or her personal information and to request the correction, destruction or deletion of his or her personal information. The employee may also on specified grounds object to the processing or further processing of personal information.

The 2018 Regulations, set out the procedure and prescribed manner in terms of which a data subject may apply for the correction, destruction or deletion of personal information. The procedures and the manner to object to the processing of personal information is also prescribed in the regulations. For example, the objection to processing personal information must be submitted on Form 1 annexed to the 2018 Regulations.

POPI generally does not apply to the processing of personal information in the workplace that has been de-identified or relates to the functions of a court.

The eight conditions for lawful processing apply to the workplace activities in various ways.

Condition 1: Accountability

The employer must ensure that the conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself. Employers must appoint an information officer who is someone duly authorised by the employer. The employer must register with the Regulator the information officer who is responsible for compliance by the employer with the provisions of POPI, working with the Regulator and dealing with requests from employees relating to their personal information.

POPI sets out the responsibilities of the information officer. These include encouraging compliance with the conditions for the lawful processing of personal information.

The 2018 Regulations set out additional responsibilities for information officers. Amongst these is that the information officer must ensure:

- The development, implementation, monitoring and maintenance of a compliance framework
- That a personal information impact assessment is done
- A manual is developed, monitored, maintained and made available as prescribed in s14 and s51 of the Promotion of Access to Information Act, No 2 of 2000
- The development of internal systems together with adequate systems to process requests for information or access thereto
- Internal awareness sessions are conducted regarding POPI, regulations in terms of POPI, codes of conduct and information received from the regulator

Condition 2: Processing limitation

Processing of personal information must be limited to lawful processing in a reasonable manner that does not infringe the privacy of the employee. The purpose of processing must be adequate, relevant and not excessive and with the consent of the employee which consent may under certain circumstances be withdrawn.

Processing is limited amongst others to protect or pursue legitimate interests or is necessary for the proper performance of a public law duty of an employer in the public service.

Personal information must be obtained directly from the applicant for employment or employee unless the information is derived from a public record or the employee has consented to the use of another source or has made the information public on for instance social media.
The processing limitation is especially relevant to the verification of information furnished by applicants for positions when only relevant and adequate information should be sought and verified.

**Condition 3: Purpose specification**

When collecting personal information it must be for a specific, explicitly defined and lawful purpose related to a function or activity of the employer in the employment context.

The employer must inform the applicant or employee of the purpose.

Without the consent of an employee an employer may only retain records of personal information for as long as it is necessary to achieve the specific purpose for which the information was collected. Pre-employment records and information should be destroyed when it does not serve any further purpose although the results of the vetting and verification may be retained for longer.

Employers must however comply with statutory provisions prescribing retention periods such as records for tax compliance and in terms of employment legislation.

The destruction of records must be final and in a manner that the records cannot be reconstructed.

**Condition 4: Further processing limitation**

Employers may with the consent of an employee put personal information to further use. In the absence of specific consent for the further use the employer may use the personal information if it is compatible with or in accordance with the purpose for which it was collected in the first place. An employer must comply with the test for compatibility when for instance passing personal information to a medical aid or retirement fund, for unemployment benefits or in a business transfer transaction.

**Condition 5: Information quality**

An employer must take reasonably practical steps to ensure that personal information of employees is complete, accurate, not misleading and updated where necessary. The employer must always have regard to the purpose for which the information was collected. Special care is required where information is collected form a source other than the employee personally.

**Condition 6: Openness**

An employer collecting personal information must take reasonably practical steps to ensure that the employee is aware of the information collected and the source of the information, the name and address of the responsible party, the purpose for which it is collected, whether the employee is obliged to supply the information and what law if any prescribes the disclosure of the information to the employer.

The employer must also inform the employee exactly what information will be processed, to whom and the employee’s right to access and rectify the information collected or to complain to the Regulator.

The employer is obliged to inform the employee before the information is collected from the employee and in any other case either before or as soon as reasonably practicable after collection.

When the employer intends to transfer the information cross border it must inform the employee and also explain to the employee the protection that the information will have in the foreign country or with the international organisation.

**Condition 7: Security Safeguards**

An employer must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of or damage to or unauthorised destruction, unlawful access to or processing of personal information.

The reasonable measures to protect the personal information include identification of possible security risks, establish and maintain safeguards against the risks, verify the safeguards from time to time and update those measures. Virus programmes, back-ups and off-site storage are all measures to consider.

The measures must comply with generally accepted information security practices.

For instance when an employer appoints a payroll administrator it must contractually oblige the administrator or any other third party to comply with the security safeguards and report to the employer any security breach.

Where there are reasonable grounds to belief that the personal information of an employee has been accessed or acquired by any unauthorised person the employer must notify the Regulator and in a prescribed form also the affected employee.

**Condition 8: Employee participation**

An employee has the right to know what personal information of him or her the employer holds.

An employee has a right in the prescribed form to request the records or a description of the personal information that the employer holds. An employee is also entitled to know which third parties have or had access to the personal information.

Upon request the employer must furnish the records or information unless the employer may rely on one of the grounds in the Promotion of Access to Information Act to refuse the record or information.

POPI applies to any personal information entered into any record by an employer.
WHAT IS AUTOMATED DECISION MAKING, AND HOW IS IT AFFECTED BY POPI?

Using software to create a personal profile of the employee in respect of performance, attendance, reliability, location, health, personal preferences or conduct would amount to automated decision-making. An employee may not be subject to a decision which results in legal consequences for or to a substantial degree affects the employee if the decision is based solely on the automated processing of personal information.

An employee may consent to automated decision-making and a contract of employment may justify a lawful process. It is also lawful when measures are in place to adequately protect the employee’s interests.

CAN EMPLOYERS PROCESS EMPLOYEE INFORMATION OUTSIDE OF THE BORDERS OF SOUTH AFRICA?

To the extent that an employer has a valid reason to process employees' personal information outside of the borders of South Africa, the employer should ensure that one of the exceptions to the general prohibition against such processing of information, set out in s72 of POPI, applies. It is possible to process personal information in this manner, with the employee’s permission, as well as for a limited list of valid operational reasons, such as that the transfer of information is necessary for the performance of a contract between the employee and the employer, or for the implementation of pre-contractual measures taken in response to the employee’s request.

Remember that when seeking an employee’s consent to deal with personal information, that the purpose specification condition explained above must be complied with.

HOW SHOULD EMPLOYERS DEAL WITH INFORMATION ABOUT TRADE UNION MEMBERSHIP?

One form of special personal information, relates to Trade Union membership. As a result, special care should be taken by employers when dealing with such information. Trade unions itself may process members' personal information, but only to the extent that it is necessary to achieve the aims of the trade union (or relevant trade union federation). Employers may find legislative
authority for dealing with trade union membership information, for instance in order to process instructions to pay trade union dues, by reason of the fact that it is doing so in order to establish, exercise or defend a right or obligation in law (s27(1)(b)), however, no processing beyond such limits will be lawful. It is advisable to seek the relevant employee’s permission (explaining the purpose) to process such information.

HOW SHOULD EMPLOYERS DEAL WITH EMPLOYMENT REFERENCES?

Employers often require certain reference checks prior to employing a person. This may include criminal or other background checks, as well as references from previous employers.

When seeking these references, employers will have to comply with POPI, in respect of the initial acquisition of the information, the storing or other processing of the information obtained thereafter, and when it eventually provides references to some future employer.

POPI does allow for the references to be obtained or granted, however employers should take into account that the criminal behaviour and biometric information a data subject are forms of special personal information, and one of the s35 exceptions must be applicable before the information may be sought and processed. Again, seeking the permission of the data subject, or making the relevant checks part of the contract of employment (eg as a suspensive condition) will serve as sufficient justification to process the information. Take into account further that s33 of POPI enjoins employers to act with such information in accordance with the prescripts of labour law.

WHAT DOES AN EMPLOYER HAVE TO DO TO BE POPI COMPLIANT?

- Appoint an information officer
- Conduct an analysis of the personal information collected and retained in the process from recruitment to retirement having regard to the eight conditions paying special attention to:
  - The purpose for the collection of the information
  - The sources of and the quality of the information
- What the information is used for
- Why records are retained and for how long
- The security measures to protect the information
- The consents on record
- What constitutes special personal information and how it is treated
- Conduct a risk assessment on the measures to protect personal information
- Revisit their HR and communication policies to ensure compliance with POPI
- Ensure that their contractual arrangements with third parties to whom they supply personal information are adequate
- Provide training to their employees on compliance with POPI
- Put in place procedures for employees to gain access to their personal information
- Revise contracts of employment to provide for consent to process personal information and for further processing
- Establish adequate policies and procedures to comply with the eight conditions

2018 REGULATIONS

The 2018 Regulations also set out the procedure for a person to submit a complaint to the Information Regulator. Form 5 annexed to the regulations can be used for such purposes.

On receipt of the complaint, the Information Regulator may take a number of actions including, among others, conducting a pre-investigation, acting as a conciliator or conducting an investigation. The 2018 Regulations set out what the Information Regulator must do if it decides to act as a conciliator and convene a conciliation meeting or if it decides to conduct a pre-investigation. The 2018 Regulations also set out the Information Regulator’s responsibilities of informing parties of developments regarding investigations.

CONSEQUENCES OF NON-COMPLIANCE

POPI creates various criminal offences for non-compliance, infringements or breach of confidentiality. The regulator may impose an administrative fine not exceeding R10 million. Some offences attract imprisonment not exceeding 10 years with or without a fine.
MARKET RECOGNITION

Our Employment team is externally praised for its depth of resources, capabilities and experience. 


The way we support and interact with our clients attracts significant external recognition.


Best Lawyers International 2019 listed Jose Jorge for employee benefits law.


ILO Client Choice Awards 2015–2016 named Michael Yeates the exclusive South African winner in the employment & benefits category. In 2018, he was named the exclusive South African winner in the immigration category.