



# THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013



Scan the QR code  
to view our team  
OR

[Click here to view](#)

## THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

### Application in the workplace

**When did the protection of personal information act 4 of 2013 (popi) commence? How long do responsible parties have to comply with its provisions?**

Certain sections of POPI commenced in April 2014. These sections relate to the definitions contained in POPI, the Information Regulator, as well as the regulations and procedures for making regulations in terms of POPI. The remaining sections of POPI commenced on 1 July 2020, save for the sections related to the amendment of laws and the functions of the Human Rights Commission.

Responsible parties have been granted a grace period of 12 months, commencing on 1 July 2020, to achieve compliance with POPI's obligations relating to the processing of personal information and special personal information. All responsible parties must therefore ensure that by 30 June 2021, all measures are in place to comply with the provisions of POPI.

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

### What is the purpose of POPI?

The preamble to POPI records that POPI emanates from section 14 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.

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

## 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 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.

## Are there exceptions to the application of POPI?

In terms of section 6 of POPI, the following instances of processing personal information are specifically excluded from its application: (i) in the course of purely personal or household activities; (ii) information that has been de-identified to the extent that it cannot be identified again; and (iii) by or on behalf of a public body which involves *inter alia*, national security, defence or public safety and identification for the purpose of identification of those involved in money laundering or terrorism. Section 7 of POPI also includes other exclusions for journalistic, literary or artistic purposes.

## 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, 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 covered by POPI includes 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.



POPI applies to any personal information entered into any record by an employer.

### 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. Special personal information processed by an employer might typically be about an employee's physical or mental health as a part of medical records, records obtained as part of a pre-employment medical questionnaire or examination, various drug or alcohol test results, sick leave records, pre-employment screening records relating to criminal convictions and any aspect of special personal information.

### Are there exceptions to the processing of special personal information?

Yes. The first exception being consent. Where a data subject consents to the processing of their special personal information, a responsible party is permitted to process the special personal information.

POPI also provides that religious or philosophical beliefs of a data subject may be processed if it is done by spiritual or religious organisations and if necessary to achieve their aims and principles. By way of example, a church is permitted to request prospective employees to provide information regarding their religious and spiritual beliefs, as this information is important for determining compatibility with the views and beliefs of the religious organisation.

In respect of race or ethnic origin, the prohibition on the processing of such information does not apply if the processing is carried out to primarily identify the data subject in compliance with applicable legislation.

Furthermore, information regarding a data subjects' health or sex life can be processed if necessary, for the implementation of the provisions of law or for the reintegration of, or support for workers or persons entitled to benefits in connection with sickness or incapacity.

Employers should be guided by the eight conditions for lawful processing of personal information and only require a data subject to disclose information which is relevant and is necessary to achieve the purpose for which it is being collected.

### **'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 job 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 persons must be dealt with in accordance with POPI.

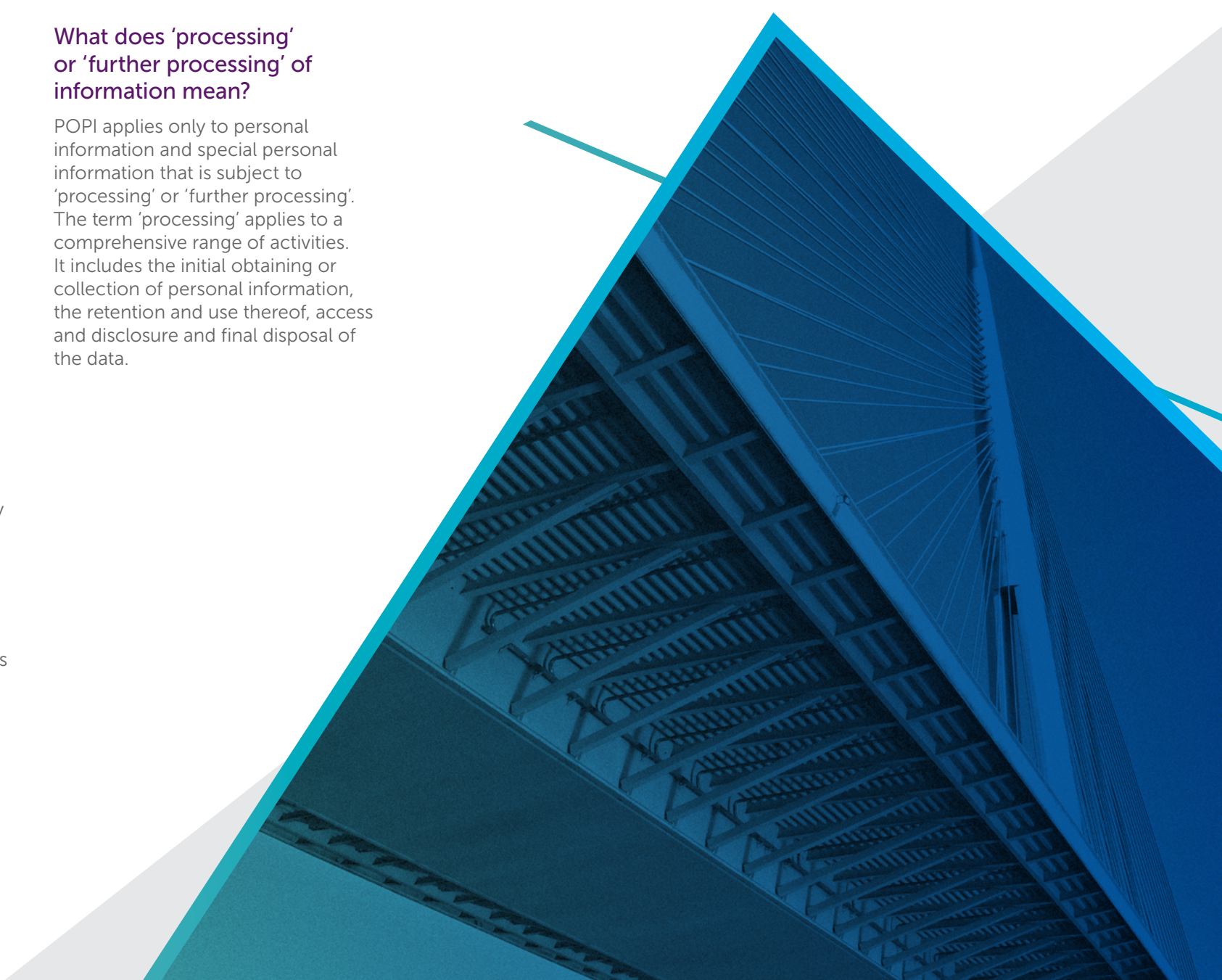
### **What manifestations of information are covered by POPI?**

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 falls within the scope of POPI, subject to limited 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 or collection of personal information, the retention and use thereof, access and disclosure and final disposal of the data.



## 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 for the processing of information specified in POPI. An employee (data subject) has the right to have his or her personal information processed in accordance with these conditions.



An employee, in addition, has the right to access 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 2018 Regulations. For example, the objection to processing personal information must be submitted on Form 1 which is annexed to the 2018 Regulations.

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

## Eight conditions for lawful processing of personal and special personal information

The eight conditions for lawful processing of personal information 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 also appoint an information officer who will be responsible for overseeing compliance with the provisions of POPI.

In the context of a juristic person, information officer means the Chief Executive Officer or equivalent officer of the juristic person. 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. The appointed and registered information officer must conduct a personal information impact assessment to ensure that the employer has adequate measures and protocols in place to comply with the conditions of lawful processing of personal information. The role and function of the information officer are dealt with more fully below.

### 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. For example, an employer is permitted to require a prospective employee to provide proof of qualification and if necessary, verify the qualification with the relevant institution but the employer will not be entitled to anything more than confirmation.

### 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.

Where an employer collects information pertaining to an employee's health as part of an incapacity enquiry as envisaged in Schedule 8 of the Labour Relations Act 66 of 1995 (LRA), the employer cannot use said information for any other purpose except that for which it was collected. As such, the employer cannot process or disclose the information except with the consent of the employee or as required by law.

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, or the information re-identified.

An employee has the right to know what personal information relating to the employee the employer holds.

#### 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 from the employee 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 on personal information to a medical aid or retirement fund, for unemployment benefits or in a business transfer transaction. For example, during the transfer of a business as a going concern in terms of section 197 of the LRA, the old employer is permitted to disclose personal information about its employees to the new employer as required by law.

#### 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 from a source other than the employee personally.

An employer must ensure that the information collected from an employee is complete, accurate and continually updated where necessary.

This means that an employer should verify the information received through documentary proof, collected with an employee's consent.

#### 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 believe 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 the employer holds pertaining to him/her.

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 2 of 2000 (PAIA) to refuse the record or information.

An employee is entitled to request a correction of any personal information. The employer must inform the employee what action has been taken pursuant to the request for a correction. The employer must correct or delete the information subject to a

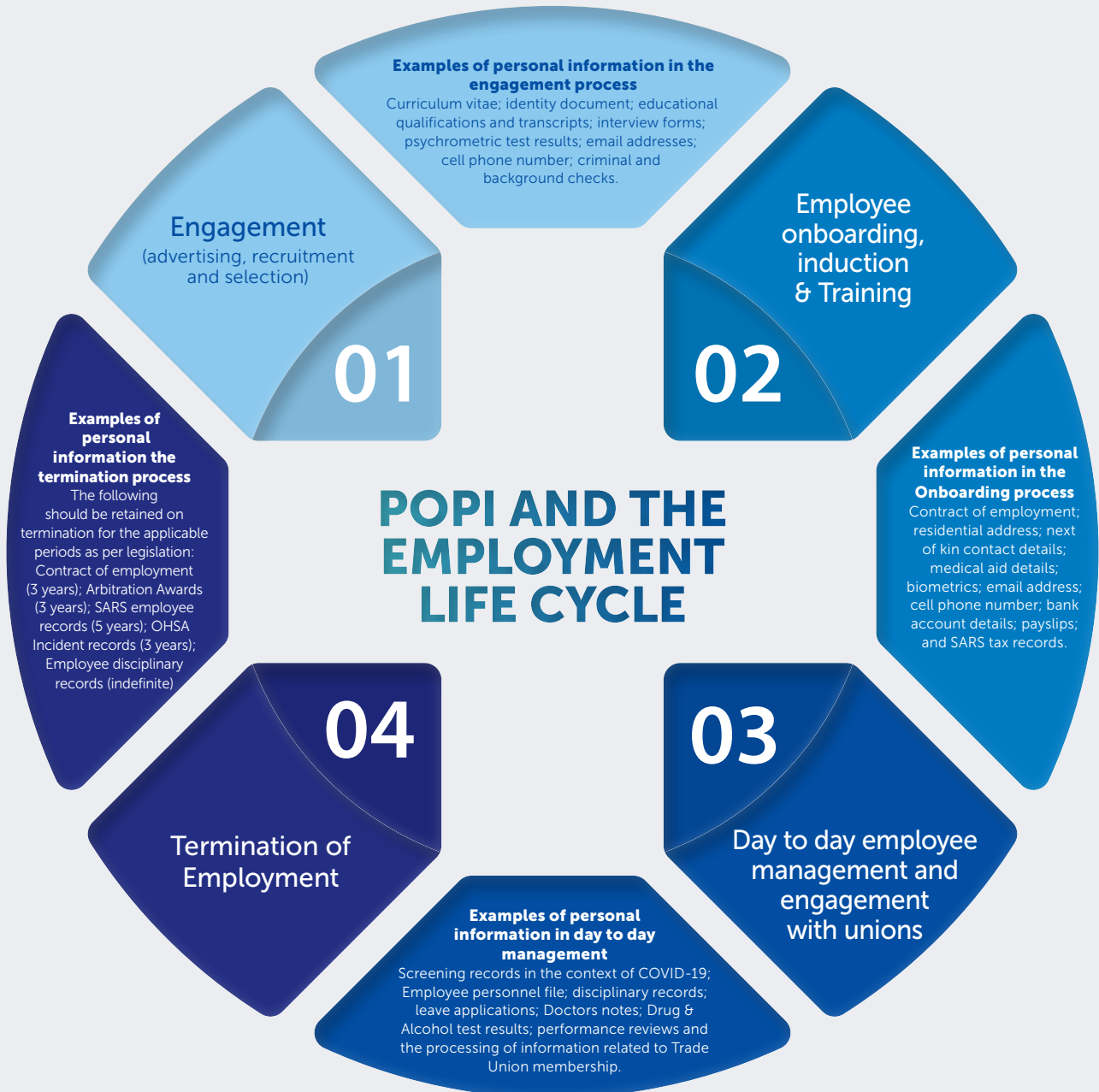
request for correction or provide proof of the correctness of the information and attach a note to the record reflecting both the request and the response. For instance, if an employee has recently wed and changes his/her surname, the employee can request the employer to update their personal information in this regard. The employer will be required to inform the employee of the actions taken pursuant to the request and provide proof of the update to his/her personal information.

The eight conditions apply to the processing of personal information in the process from recruitment to retirement and oblige employers at each stage to consider carefully the purpose for collecting the information, why it should be retained and for how long, what they may use the information for and the obligation to grant employees access to the information.

The following non-exhaustive list, is potential personal information which an employer is likely to process during an employee's employment lifespan.

## PERSONAL INFORMATION AND THE EMPLOYMENT LIFE CYCLE

# POPI AND THE EMPLOYMENT LIFE CYCLE



# 01

## Notes for the engagement process:

the personal information of applicants must be obtained directly from them. However, in an instance when an employer makes use of LinkedIn, the information need not be collected directly from the applicant as it would be derived from a public platform, and the personal information would have been made public by the applicant. Where an employer makes use of a recruitment agency, the applicant must consent to his/her personal information being obtained from the recruitment agency.

The personal information of unsuccessful applicant(s) must be destroyed once a decision has been taken not to employ the applicant(s) as the purpose for which the personal information was collected ceases to exist, unless the applicant requests that the employer retains the information.

# 02

## Notes for the induction and induction process:

there are many forms and documents in the onboarding process that require information regarding an employee's next of kin's personal information including inter alia, their identity number, contact details and physical address. The nature of the information required pertaining to a next of kin constitutes 'personal information' in terms of POPI, as it is information related to an identifiable, living, natural person.

The provisions of POPI must therefore be adhered to in relation to this information. Accordingly, an employer must (i) notify the next of kin that their personal information is being processed and (ii) only process personal information pertaining to a next of kin with their consent. The onus of proof rests with the employer to prove that consent was received from a next of kin.

# 03

## Notes for day-to-day management of employees:

The following actions are recommended in order to ensure compliance with POPI in the day to day management of employees:

- Ongoing analysis of personal information collected to verify the quality, accuracy and completeness of the information;
- Conduct risk assessments to determine where the company falls short of their obligations to comply with POPI;
- Revise HR policies to ensure compliance with POPI;
- Revise and update contractual arrangements to ensure compliance with POPI; and
- Procedures must be put in place for employees to access their personal information.

# 04

## Notes for termination of employment:

Save for the information that must be retained in terms of applicable legislation, an employer must undertake the disposal of personal information in line with section 14 of POPI where an employment relationship is terminated.

There is no stipulated time period set out in POPI for the destruction and disposal of records of personal information, except that this must happen as soon as reasonably practicable after the employer is no longer authorised to retain the record.

Once the employer has disposed of the records of personal information of employees, it should no longer have access to it. As such personal information stored online should be deleted from all hard drives and servers, whilst all hard copies should also be destroyed in an appropriate manner. Personal information retained for further processing in terms of section 15(e) of POPI must be processed solely for that purpose and should not be published in an identifiable form.



POPI contains specific provisions regulating the processing of special personal information.

### **What additional requirements are applicable to the processing of special personal information?**

POPI contains specific provisions regulating the processing of special personal information.

An employer may not process special personal information without the consent of the employee unless processing is necessary for the establishment, exercise or defence of a right or obligation in law or the employee has already made the information available for instance on social media. The regulator may also authorise processing of special personal information if it is in the public interest and subject to appropriate safeguards. The employer may also rely on any of the listed exceptions.

Special exemptions apply to the processing of personal information concerning an employee's religious or philosophical beliefs.

The special personal information concerning race or ethnic origin may without consent be used to comply with legislation.

An employer may without consent process special personal information concerning the health of an employee if it is necessary for the administration of retirement funds and medical schemes or to reintegrate or support employees entitled to incapacity or ill health benefits.

Employers may without consent process special personal information to comply with collective bargaining obligations.

### **How is an information officer appointed and their duties?**

Responsible parties must appoint an information officer who will be responsible for overseeing compliance with the provisions of POPI. Information Officers are, by virtue of their positions, appointed automatically in terms of PAIA and POPI. An information officer in the context of a juristic person means the Chief executive officer or equivalent officer of the juristic person. The Information officer of a responsible party must be registered with the Information Regulator in terms of the registration form made available by the regulator.

POPI sets out the duties and responsibilities of an Information Officer's duties which, amongst others, include:

- 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 section 14 and section 51 of the PAIA
- The development of internal systems together with adequate systems to process requests for information or access thereto
- Internal awareness sessions are conducted regarding POPI, 2018 Regulations in terms of POPI, codes of conduct and information received from the regulator

### How does POPI apply to COVID-19 related information?

The information Regulator issued a Guidance Note to give effect to the right to privacy as it relates to the protection of personal information of data subjects for the purpose of managing the spread of COVID-19. The Guidance Note outlines the conditions for the lawful processing of personal information in order to detect, contain and prevent the spread of COVID-19.

Although, employers are permitted to request from employees specific information on the health status of the employee in the context of COVID-19, in line with the employer's obligation to maintain a safe and hazardous free working environment in terms of the Occupational Health and Safety Act 85 of 1993 read together with the Employment Equity Act 55 of 1998. Employers must still comply with the eight conditions of lawfully processing information, in that they must, *inter alia*, put in place adequate security measures to ensure the integrity and confidentiality of personal information of data subjects and to destroy or delete the information when no longer authorised to retain it.

The Guidance Note confirms that responsible parties are not required to obtain the employee's consent prior to the processing of person information in the context of COVID-19 as the processing of such information is in compliance with the responsible parties legal obligations and is in line with the public interest as per the exceptions set out in section 27 of POPI.

Employers can further process personal information, notwithstanding the fact that such processing is not compatible with the original purpose, if it necessary to prevent a serious and imminent threat to public safety or public health, the life or health of an employee or another.

### 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 section 72 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, 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. A 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 (section 27(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 section 36 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 (e.g. as a suspensive condition) will serve as sufficient justification to process the information. Take into account further that section 33 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 Law team is externally praised for its depth of resources, capabilities and experience.

*Chambers Global 2014–2024* ranked our Employment Law practice in Band 2 for employment. *The Legal 500 EMEA 2020–2024* recommended the South African practice in Tier 1. *The Legal 500 EMEA 2023–2024* recommended the Kenyan practice in Tier 3 for employment.

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

**Aadil Patel** is the Practice Head of our Employment Law team, and the Head of our Government & State-Owned Entities sector. *Chambers Global 2024* ranked Aadil in Band 1 for employment. *Chambers Global 2015–2023* ranked him in Band 2 for employment. *The Legal 500 EMEA 2021–2024* recommended Aadil as a 'Leading Individual' for employment and recommended him from 2012–2020.

*The Legal 500 EMEA 2021–2024* recommended **Anli Bezuidenhout** for employment.

*Chambers Global 2018–2024* ranked **Fiona Leppan** in Band 2 for employment. *The Legal 500 EMEA 2022–2024* recommend Fiona for mining. *The Legal 500 EMEA 2019–2024* recommended her as a 'Leading Individual' for employment, and recommended her from 2012–2018.

*Chambers Global 2021–2024* ranked **Imraan Mahomed** in Band 2 for employment and in Band 3 from 2014–2020. *The Legal 500 EMEA 2020–2024* recommended him for employment.

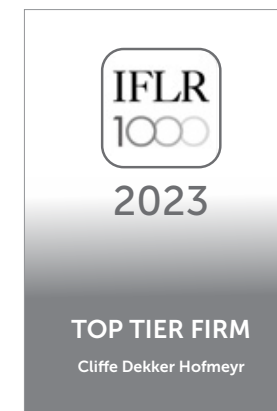
*The Legal 500 EMEA 2023–2024* recommended **Phetheni Nkuna** for employment.

*The Legal 500 EMEA 2022–2024* recommended **Desmond Odhiambo** for dispute resolution.

*The Legal 500 EMEA 2023* recommended **Thabang Rapuleng** for employment.

*Chambers Global 2024* ranked **Njeri Wagacha** in Band 3 for FinTech. *The Legal 500 EMEA 2022–2024* recommended Njeri for employment.

*The Legal 500 EMEA 2023–2024* recommends her for corporate, commercial/M&A.



**BBBEE STATUS:** LEVEL ONE CONTRIBUTOR

Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

**PLEASE NOTE**

This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

**JOHANNESBURG**

1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa.  
Dx 154 Randburg and Dx 42 Johannesburg.  
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E [jhb@cdhlegal.com](mailto:jhb@cdhlegal.com)

**CAPE TOWN**

11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.  
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E [ctn@cdhlegal.com](mailto:ctn@cdhlegal.com)

**NAIROBI**

Merchant Square, 3<sup>rd</sup> floor, Block D, Riverside Drive, Nairobi, Kenya. P.O. Box 22602-00505, Nairobi, Kenya.  
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114  
E [cdhkenya@cdhlegal.com](mailto:cdhkenya@cdhlegal.com)

**NAMIBIA**

1<sup>st</sup> Floor Maerua Office Tower, Cnr Robert Mugabe Avenue and Jan Jonker Street, Windhoek 10005, Namibia  
PO Box 97115, Maerua Mall, Windhoek, Namibia, 10020  
T +264 833 730 100 E [cdhnamibia@cdhlegal.com](mailto:cdhnamibia@cdhlegal.com)

**STELLENBOSCH**

14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.  
T +27 (0)21 481 6400 E [cdh Stellenbosch@cdhlegal.com](mailto:cdh Stellenbosch@cdhlegal.com)

©2025 0781/JAN

