

<p><b>SUMMARY OF</b></p> <p><b>THE PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 (POPIA)</b></p>
--

**WHO DOES THE ACT APPLY TO?**

POPIA regulates the “processing” of personal information in South Africa, including the processing of personal information that is entered in a record, by a private or public body that is domiciled in SA, or a private or public body that is domiciled elsewhere but uses automated or non-automated means situated in South Africa.

**KEY DEFINITIONS**

**“Processing”** - includes collecting, receiving, recording, organising, retrieving, or using such information; or disseminating, distributing or making such personal information available. The Act will also relate to records which you already have in your possession.

**“Consent”** – any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

**“Data Subject”** – you or me, the person to whom personal information relates.

**“Direct Marketing”** – sending a data subject an electronic communication about goods and services that you are promoting or offering to supply in the ordinary course of business, or requesting a donation of any kind for any reason.



**“Processing”** – any operation or activity concerning personal information.

**“Record”** – any recorded information, regardless of the form or medium, or when it came into existence.

**“Responsible Party”** – a public or private body or any other person which alone or in conjunction with others, determines the purpose of and means for processing personal information.

**“Operator”** – a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

**“Personal Information”** - is defined in Section 1 of the POPIA and means information relating to an identifiable, living natural person, and where it is applicable, an identifiable, existing juristic person and includes (but is not limited to) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person; and the name of a person if it appears with other personal information relating to the person or of the disclosure of the name itself would reveal information about the person.

Date updated	Updated by	Signed	Information Officer Approval	Page 1 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

**“Special Personal Information”** – section 26 of the Act: A responsible party may, subject to section 27, not process personal information (special personal information) concerning: religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject. A Responsible Party is not allowed to process this special personal information unless it is done with consent; or is necessary in law; or is done for historical, statistical or research purposes; or the information has been deliberately made public by the data subject.



**POPIA PROVIDES FOR 8 CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION IN SECTION 4**

- (1) **Accountability:** The responsible party must ensure that the conditions and all the measures set out in the Act that give effect to such conditions, are complied with at the time of the determining of the purpose and form of the processing of personal information. (section 8)
- (2) **Processing limitation:** personal information may only be processed in a fair and lawful manner and only with the consent of the data subject. (sections 9 – 12)
- (3) **Purpose specification:** personal information may only be processed for specific, explicitly defined and legitimate reasons. (sections 13 – 14)
- (4) **Further processing limitation:** personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose. (section 15)
- (5) **Information quality:** The responsible party must take reasonable steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary. (section 16)
- (6) **Openness:** The data subject whose information are being collected must be aware that you are collecting such personal information and for what purpose the information will be used. (sections 17 – 18)
- (7) **Security safeguards:** personal information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorized destruction and disclosure. (sections 19 – 22)
- (8) **Data subject participation:** Data subjects may request whether their personal information is being held by a particular business. They may also request the correction or amendment of their personal information or the deletion thereof from the business’ records. (section 23 – 25)

Compliance in terms of these conditions is required and translates to the proper management, retention and disposal of records. In order to achieve this compliance goal, a business should develop and adopt a plan or programme which is structured. This plan will have to be in the form of a manual which should be accessible to any person who wishes to see in what manner your business deal with personal information.

**WHAT ARE THE RIGHTS OF A DATA SUBJECT?**

A Data Subject have the right to:

Date updated	Updated by	Signed	Information Officer Approval	Page 2 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

- be told if someone is collecting his personal information
- if his personal information has been accessed by an unauthorised person
- access his personal information
- require that his personal information to be corrected or destroyed
- object to his personal information being processed.

**EXCLUSIONS (INSTANCES WHERE THE ACT DOES NOT APPLY)**

The Act does not apply to:

- personal information processed in the course of a personal or household activity;
- personal information that has been de-identified to the extent that it cannot be re-identified;
- where the processing authority is a public body involved in national security, defence, public safety, anti-money laundering, or the Cabinet or Executive Council of the province or as part of a judicial function.

**PERSONAL INFORMATION CAN ONLY BE PROCESSED: – (SECTION 11)**



- with the consent of the data subject; or
- if it is necessary for the conclusion or performance of a contract to which the data subject is a party; or
- it is required by law; or
- it protects a legitimate interest of the data subject; or
- it is necessary to pursue your legitimate interests or the interest of a third-party to whom the information is supplied.

**A RESPONSIBLE PARTY HAS TO COLLECT PERSONAL INFORMATION DIRECTLY FROM THE “DATA SUBJECT”, UNLESS:**

- This information is contained in some public record or has been deliberately published by the data subject;
- collecting the information from another source does not prejudice the data subject;
- it is necessary for some public purpose; or to protect the interests of the responsible party;
- obtaining the information directly from the data subject would prejudice a lawful purpose or is not reasonably possible.

**PURPOSE OF COLLECTION:**

- The Responsible Party can only collect personal information for a specific, explicitly defined and lawful purpose and the data subject must be aware of the purpose for which the information is being collected. (section 13)
- Once the personal information is no longer needed for the specific purpose, it must be disposed of (the subject must be “de-identified”), unless the Responsible Party

Date updated	Updated by	Signed	Information Officer Approval	Page 3 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

needs to keep it (or are allowed to keep it) by law, or need to keep the record for his own lawful purpose or in accordance with the contract between himself and the data subject, or the data subject has consented to the Responsible Party keeping the records. (section 14)



- The Responsible Party is entitled to keep records of personal information for historical, statistical or research purposes if he has established safeguards to prevent the records being used for any other purposes.
- The Responsible Party can only use personal information collected, for the purpose which it was collected for. (section 15)
- If a responsible party wishes to process personal information for a purpose other than for which the information was collected with the intention of linking the information to information processed by others, such a person will need to get prior authorisation from the Regulator. (section 15 (3) (d) (f) and section 37). Such prior authorisation will also be needed for processing information on criminal, unlawful or objectionable conduct or credit reporting. Failure to obtain such prior authorisation would be a criminal offence.

**NOTIFICATION AND INFORMED CONSENT REQUIRED WHEN COLLECTING PERSONAL INFORMATION:** (Section 18)

The data subject must be made aware of the following:

- the information that is being collected, and if the information is not being collected from the subject, the subject must be made aware of the source from which the information is being collected;
- the name and address of the person/organisation collecting the information;
- the purpose of the collection of information;
- whether the supply of the information by the subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- whether the information is being collected in accordance with any law;
- if it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa;
- who will be receiving the information;
- that the subject has access to the information and the right to rectify any details;
- that the subject has the right to object to the information being processed (if such right exists);
- that the subject has the right to lodge a complaint to the Information Regulator. The contact details of the Information Regulator must also be supplied.

These requirements have to be met before the information is collected directly from the subject, or soon as reasonably practicable thereafter if the information is not collected directly from the subject, unless the subject is already aware of these rights. If you collect additional information from a subject for a different purpose, you have to go through this process again. S18(3)

Date updated	Updated by	Signed	Information Officer Approval	Page 4 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

## HOW SHOULD A RESPONSIBLE PARTY HANDLE PERSONAL INFORMATION COLLECTED?

Anybody who keeps personal information has to take steps to prevent the loss, damage, and unauthorised destruction of the personal information. They also have to prevent unlawful access to or unlawful processing of this personal information. (section 19)

A Responsible Party has to identify all risks and then establish and maintain safeguards against these identified risks. The Responsible Party have to regularly verify that the safeguards are being effectively implemented and update the safeguards in response to new risks or identified deficiencies in existing safeguards.

## RESPONSIBILITIES OF EMPLOYEES AND OPERATORS

Anybody processing personal information on behalf of a Responsible Party must have the necessary authorisation from the Responsible Party to do so. They must also treat the personal information as confidential. (section 20)

Such a person or business (Employee or an “Operator”) must have a written contract with the Responsible Party in which they are specifically obliged to maintain the integrity and confidentiality of the personal information and to implement the established safeguards against identified risks.

This Operator is also obliged to notify the Responsible Party if they believe that personal information has been accessed or acquired by an unauthorised person (section 21(2))

## DATA BREACHES

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator as well as the data subject (if the data subject can still be identified) of the data breach. (section 22)



## PERSONAL INFORMATION OF CHILDREN

Special rules apply to the processing of personal information of children. (section 35)

## EXEMPTION FROM CONDITIONS FOR PROCESSING OF PERSONAL INFORMATION

The Information Regulator has the power to grant exemptions to allow people to process personal information without complying with the Act if the public interest outweighs the data subject’s rights of privacy or where there is a clear benefit to the data subject. Such exemptions may be granted upon conditions. (section 37)

Exemptions may also be granted for the processing of personal information for the purposes of discharging a “relevant function”. A relevant function would include the processing of personal information with a view to protecting members of the public against: (i) financial loss due to dishonesty of persons in the banking or financial services industry; and (ii) dishonesty by persons authorised to carry on any profession or other activity. (section 38)

Date updated	Updated by	Signed	Information Officer Approval	Page 5 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

## RIGHTS OF DATA SUBJECTS REGARDING DIRECT MARKETING

Section 69 of the Act outlaws direct marketing by means of any form of electronic communication unless the subject has given their consent. Such an electronic communication obviously includes emails and SMSs. Automatic calling machines are also included. A subject can only be approached once to obtain such a consent. Once such consent is refused, it is refused for ever. (section 69 (1) and (2))

Slightly different rules apply if the data subject is a customer. Here the customer's contact details must have been obtained in the context of the sale of a product or a service, the direct marketing by electronic communication can only relate to the suppliers own similar products or services, and the customer must have been given the right to opt out at the time that the information was collected and each time such a communication is sent. (section 69 (3))

Anybody sending out direct marketing electronic communications has to disclose the identity of the advertiser and provide an address to which the customer can send a request to opt out. (section 69 (4))

Any data subject whose name is included in any type of directory must be advised of the purpose of the directory and about any future uses to which the directory might possibly be put, based on search functions embedded in electronic versions of the directory. Such a subject must be given the opportunity to object to such use of the personal information. This will however not apply to directories that were printed or which were created in off-line electronic form prior to the commencement of this section. (section 70)

If your personal information is contained in a public subscriber directory which has been prepared in accordance with the safeguards set out in the Act, prior to the commencement of this portion of the Act, your personal information can remain in the directory provided that the data subject has received notification about the purposes of the directory and the future uses to which the directory might be put. Again, the data subject must be given the opportunity to opt out. (section 70)



## THE INFORMATION OFFICER

An Information Officer needs to be appointed by every responsible party. The duties and responsibilities of the Information Officer is stipulated in the Act as follows:

### Section 55 - DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER

- Encouragement of compliance, by the responsible party with the conditions of the processing of personal information;
- Dealing with requests made to the responsible party pursuant to POPIA;
- Working with the Information Regulator in relation to investigations conducted pursuant to Chapter 6 of the Act.

Provision is made for the appointment of Deputy Information Officers should it be necessary.

Date updated	Updated by	Signed	Information Officer Approval	Page 6 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

## Regulation 4 - DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICERS

Subject to the provisions of section 55 of the Act, an information officer must ensure that—

- a compliance framework is developed, implemented and monitored;
- adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- preliminary assessments are conducted;
- a manual for the purpose of the Promotion of Access to Information Act and the Act is developed detailing the purpose of the processing; a description of the categories of data subjects and of the information or categories of information relating thereto; the recipients or categories of recipients to whom the personal information may be supplied; the planned trans-border or cross border flows of personal information; and a general description allowing preliminary assessment of the suitability of information security measures to be implemented and monitored by the responsible party;
- the manual is available — on the website of the responsible party and at the office or offices of the responsible party for public inspection during normal business hours of that responsible party;
- internal measures are developed together with adequate systems to process requests for information or access thereto; and
- awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- The information officer, or a person designated by him or her, can upon request of any person provide copies of the manual, to that person upon payment of a fee determined by the responsible party, which may not be more than R3.50 per page.

### TRANSBORDER INFORMATION FLOWS

A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless: (Section 72)



- that third party is subject to a law, binding corporate rule or binding agreement which provide an adequate level of protection of the personal information of a data subject.
- the subject has agreed to the transfer of information;
- such transfer is part of the performance of a contract which the subject is a party; or
- transfer is for the benefit of the subject and it is not reasonably practicable to obtain their consent and that such consent would be likely to be given.

### ENFORCEMENT OF POPIA

The Office of the Information Regulator has been established with the Information Regulator appointed by the President on the recommendation of the National Assembly.

Powers, Duties and Functions of the Information Regulator are the following: (section 39 – 54)

- to provide education to the public relating to the Act and to give advice to government or private bodies as regards their obligations under the Act.

Date updated	Updated by	Signed	Information Officer Approval	Page 7 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

- to monitor and enforce compliance of the Act and to keep up-to-date with the latest developments in information processing and computer technology to ensure that this does not impact negatively on the protection of personal information.
- to monitor proposed legislation to make sure that this is in line with the Act;
- to report to Parliament on its own accord on any policy matters;
- to submit an annual report to Parliament;
- to conduct assessments as to whether any specific public or private body is complying with the Act;
- by maintaining registers that are prescribed in the Act;
- by consulting with interested parties on matters relating to personal information and mediating disputes;
- by handling complaints about violations of rights;
- by enforcing the provisions of the Act;
- by conducting research;
- by drafting codes of conduct and guidelines; (section 60 – 68) The Regulator is entitled to issue codes of conduct regarding the processing of personal information which codes of conduct may be of general or specific application. Prior to issuing such a code of conduct the Regulator has to advertise their intention and call for written submissions. These codes of conduct must be published in the Government Gazette and the Regulator must keep a register of approved codes of conduct. These codes of conduct can be reviewed and revoked from time to time.
- by facilitating cross-border cooperation to enforce privacy laws; and
- by doing anything further which they think is necessary to further the aims of the Act.
- The Information Regulator will also have an Enforcement Committee. (section 50)

## DISPUTES AND BREACHES



(Sections 73 – 99)

If someone is alleged to be in breach of the Act, any person may submit a complaint to the Information Regulator. This complaint will be dealt with by an adjudicator. From the Act it would appear that anybody can submit this type of complaint. It does not have to be one of the subjects whose rights have been breached.

If a person is not happy with the determination of the adjudicator, they can still approach the Information Regulator for another ruling.

When a complaint is referred to the Regulator, the Regulator has certain options. It can:

- conduct pre-investigation;
- act as a conciliator;
- if after investigating the complaint the Regulator believes there is no case either because of the passing of time, the trivial subject matter of the complaint, the fact that the complaint is frivolous or vexatious or not made in good faith, or if the complainant does not have a sufficient personal interest in the matter, or where there is another internal remedy which has not yet been exhausted, or where further Action would be unnecessary or inappropriate, decide to take no action;

Date updated	Updated by	Signed	Information Officer Approval	Page 8 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd



- conduct a full investigation;
- refer the complaint to the Enforcement Committee.

The Regulator also has the right to commence an investigation on their own initiative. (sections 76 & 77)

The Information Regulator can also refer any complaint to another body if the Regulator believes that the complaint falls more properly within the jurisdiction of this other body.

The Information Regulator has the right to summon people to appear before it and to give evidence. This evidence does not have to be evidence that would be admissible in a court of law.

The Information regulator can also enter and search any premises, conduct private interviews at any place or carry out other enquiries that the Regulator sees fit.

The Information Regulator is entitled to approach the judge of the High Court or a magistrate to issue a search warrant which would empower the Regulator to search, inspect, examine, operate and test any equipment used for the purposes of processing personal information on the premises of a responsible party.



The Information Regulator also has the powers of seizure in respect of evidence or prospective evidence.

It would appear that anybody is entitled to ask the Information Regulator to make an assessment as to whether an instance of processing of personal information complies with the Act. The Regulator can also do this on its own initiative. The results of the assessment must be communicated to the person who has made the request. If the Regulator deems it appropriate and in the public interest, the results of the assessment can be published. (section 89)

After completing an investigation, the Regulator may refer the complaint or other matter to the Enforcement Committee for consideration, for a finding and for a recommendation in respect of proposed remedial Action. The Regulator may prescribe the procedure to be followed by the Enforcement Committee. (section 92)

The Enforcement Committee will make recommendations to the Regulator necessary or incidental to any Action that should be taken against the responsible party.

The Information Regulator will make the final “judgement” on the complaint. The guilty party will be advised of their appeal rights. The enforcement notice may not require the responsible party to take any remedial action until the period for an appeal has passed, and if such appeal is lodged, until it has been determined. The Information Regulator does however have the power to enforce immediate compliance if the matter is viewed as urgent.

Date updated	Updated by	Signed	Information Officer Approval	Page 9 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

A guilty party has a right of appeal of to the High Court and such a party has 180 days to appeal.

A subject who has suffered damages as a result of the responsible party failing to comply with this Act can institute a civil action (or request the Information Regulator to do this on his behalf) to recover these damages whether or not there has been any intention or negligence on the part of the responsible party. This creates a strict liability on the part of the responsible party. The Act sets out a fixed number of defences that can be raised against an action for damages. These are:

- Vis major;
- consent of the plaintiff;
- fault on the part of the plaintiff (contributory negligence);
- that compliance was not reasonably practicable in the circumstances; or
- that the regulator had granted an exemption in respect of compliance.

If the responsible party is found to be guilty the court has the jurisdiction to award damages as compensation for patrimonial and non-patrimonial loss suffered by the subject and for aggravated damages, in a sum determined in the discretion of the court. The court can also order the payment of interest on damages and costs of suit on a scale as to be determined by the court.

Any amount awarded to the subject by the court must be paid to the Information Regulator and used first to defray expenses incurred by the Information Regulator in the case. Any available balance will then be paid to the data subject.

Any court issuing an order of this nature must publish such an order in the Government Gazette or by such other appropriate public media announcement as the court might consider appropriate.



## OFFENCES, PENALTIES AND ADMINISTRATIVE FINES

Sections 100 – 106 deal with instances where parties would find themselves “guilty of an offense”.

The most relevant of these are:

- Any person who hinders, obstructs or unlawfully influences the Regulator;
- A responsible party which fails to comply with an enforcement notice;
- Offences by witnesses, for example, lying under oath or failing to attend hearings;
- Unlawful Acts by *responsible party* in connection with account numbers;
- Unlawful Acts by *third parties* in connection with account numbers.

Section 107 of the Act details which penalties apply to respective offenses. For the abovementioned offences, (Section 107(a)) the maximum penalties are a fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment. For the less serious offences, (section 107(b)) for example, hindering an official in the execution of a search and seizure warrant the maximum penalty would be a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.



Date updated	Updated by	Signed	Information Officer Approval	Page 10 of 11
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd

Administrative fines may also be imposed by the Information Regulator in terms of section 109 of the Act.

## REGULATIONS

In terms of section 112 of the Act, both the Minister and the Information Regulator may make and issue regulations to the Act.

In the current Regulations, provision is made for prescribed forms to be utilised by Data Subjects when requesting amendments, corrections or deletion of personal information, or when requesting the Information Regulator to issue a code of conduct, as well as other administrative considerations. The Duties and responsibilities of the Information Officer is detailed in the Regulations.

Date updated	Updated by	Signed	Information Officer Approval	Page <b>11</b> of <b>11</b>
1 July 2021	J Smit			
Supplied by FHBC (Wellington) (Pty) Ltd				© FHBC (Wellington) (Pty) Ltd