

POPIA POLICY


PLACEMENT PERSONNEL

REVISION 2

DATE: 22 NOVEMBER 2021

DOC NR: POL-COM-006

APPROVAL

Company	Name	Policy Revision	Date	Signature
Nursetec	NCD Van Huyssteen	2	22 November 2021	

CONFIGURATION OF DOCUMENT

Revision nr:	Date:	Selection/Page adjusted:	Revised/Adjusted by:	Developed by
1	28 October 2017	N/A	Revised	A Janse van Vuuren
2	22 November	Policy in Total	A Janse van Vuuren	

1. INTRODUCTION

We live in an age where information is easily accessible, and this poses as much threat as it enables convenience. In addition to being easily accessible, data can be processed at warp speed and in high volumes at a touch of a button.

2. PURPOSE

The POPI Act exists to promote each South African's right to privacy, as stipulated in the Constitution, in addition to restraining how personal information may be processed and released. The responsibility of protecting personal information starts with each individual self. Although the act is only enforceable on legal entities, each individual is responsible for the information they give out about themselves, and those of data subjects.

This policy should be read in collaboration with the Company PAIA manual, and any other policies that may hold relevance.

3. SCOPE

This policy is applicable to all Nursetec employees that work directly or indirectly with personal information, including data subjects, Company Clients, Operators, or Service Providers

4. DEFINITIONS

4.1 Data Subject:

The person to whom the personal information, at hand, relates to

4.2 Information Officer

Is classified in the POPI Act as the head of a company

4.3 Deputy Information Officer

Employee that the Information Officer appointed in this role, to whom the Information Officer has delegated his powers and duties in terms of POPIA

4.4 Data Capturer/Handler/Responsible Party

For the purpose of this policy, the term data-capturer/handler/responsible party implies any individual that has access to, or is in charge of obtaining, processing, retaining, or destruction of any personal information, of a data subject

4.5 Regulator

Means the person appointed by the President to regulate the compliance of legal entities with the Act, in addition to receiving individual and organisational complaints

4.6 Client:

For the purpose of this Policy, the term Client pertains to any entity or individual, to which Nursetec delivers a service, or will prospectively be delivering a service in future

4.7 Personal information:

- 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 the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

4.8 Processing of personal Information:

Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, collected from data subjects, includes but is not limited to, collecting, receiving, recording, organising, collating, storing, updating, retrieving, altering, using, disseminating, distributing, merging, linking, blocking, degrading, erasing or destroying of any personal information

4.9 Transparency:

For the purpose of this policy, being transparent will signify openness – i.e., easy to perceive or detect

4.10 Body:

Means Public or Private entity

4.11 PAIA

Promotion of Access to Information Act

4.12 Third Party/Operator

Provider of the Company, which delivers a service to the Company, or on behalf of the Company, and operates under Company instruction. Third Parties may also include those serving in the Public Sector, or Private Parties contracted, delegated to monitor and audit statutory compliance.

4.13 Competent Person

Individual of age, who is legally entitled to act on behalf of a minor, or who is legally assigned to act on behalf of another individual

4.14 The Company Nursetec SA (Pty) Ltd.

5 POLICY STATEMENT

Nursetec recognises the importance of the POPI Act, and will:

- Comply with legislation
- Respect all individual rights - those of employees and the clients of the organisation, in regards to Protection of Personal Information and Promotion of Access to Information.
- Protect individual rights and be transparent with the data-subjects on what collected information will be used for
- Provide training of what can and can't be done with the implementation of POPI.
- Legitimise any and all concerns that employees or clients may have in regards to the processing of their personal information

6 EXCLUSIONS

The Act does not apply to the processing of personal information:

- In the course of a purely personal or household activity
- That has been de-identified to the extent that it cannot be re-identified again
- By or on behalf of a public body—
- which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety
- the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information
- Terrorist and related activities
- Exclusion for journalistic, literary or artistic purposes as defined in Section 7(1), (2), and (3), of the Protection of Personal Information Act

7 CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION AS DEFINED BY THE ACT

7.1 Accountability

The responsible party must ensure that the conditions set out below, and all the measures that give effect to such conditions, are complied with at the time of intend to collect, the collection itself, and during the processing of such personal information

7.2 Processing Limitation

Personal information may only be processed if:

- It is done lawfully

- Hold relevance and is not excessive
- Data subject, or competent person, consents to the processing
- Processing is in line with contractual terms and conditions
- It is a legal requirement
- Processing protects data subject interest
- Processing is necessary for the proper performance for a public law duty by a public body
- It is in the representation or pursuit of legitimate business needs

A Data Subject may:

- withdraw his/her consent, provided it does not affect legal compliance, of processing that occurred before withdrawal
- object to the processing of his/her personal information, whereafter a data handler may no longer process such information

Personal information may only be collected directly from the data subject, unless:

- The data is derived from public record, or has deliberately been made public by the data subject
- The data subject, or competent person has consented to the collection of personal information, from another source
- To avoid prejudice to the maintenance of law by a public body
- To comply with an obligation imposed by law, or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Act
- For the conduct or proceedings in any court or tribunal that have commenced or are reasonably contemplated
- It is in the interest of National Security
- To maintain the legitimate business interest of the Company, or of the third party to whom the information is supplied to
- Compliance would prejudice the lawful purpose of collection
- Compliance is not reasonably predictable in the specific case at hand

7.3 Purpose Specification

Personal information may only be processed in line with the reason for collection and it must be relevant at all times

Retention and Restriction of Records:

Records containing personal information must not be retained longer than necessary for the purpose on what the information was initially collected and processed, unless;

- Retention of record is required or authorised by law
- Company requires retention of record, for legal compliance in relation to its functions and activities
- Retention of record is required by a contract between the parties thereto
- Data subject, or competent person has consented to record retention

- Records may be retained in excess, than what it was originally collected and processed for, if, it is for historical, statistical, or research purposes, granted the Company has relevant safeguards in place

Retention Period:

- A record containing personal information must be kept for as long as prescribed by the relevant legislation
- In the even that there is no lawful prescription, record must be kept for a reasonable time, to allow the data subject, to request access to the record

Destruction or Deletion of Records:

- A record must be destroyed, or de-identified, after timeframe of which it was legally required to be retained has passed, or where there is no prescription when reasonable predicted
- The destruction or deletion must take place in such a manner that it prevent restructure in an intelligible form

Restriction on the processing of personal information:

The Processing of personal information must be restricted if;

- Its accuracy is contended by the data subject, for a period during which the data handler must verify the personal information
- The reason for collection and processing is no longer applicable, and record needs to only be retained for proof
- Processing is unlawful, and data subject opposes its destruction or deletion, and request the use of information be restricted, instead
- The data subject request the personal information be transmitted into another automated system

Personal information on which there is a processing restriction, as referred to above, may only be stored, processed for purpose of proof, processed with the consent of a data subject or competent person, or processed for the protection of rights of another natural or legal person, or in the interest of the public. In cases where there was a restriction placed on the processing of personal information, the data handler or responsible party must inform the data subject that the restriction will be lifted, before doing so.

7.4 Further Processing Limitation

Further processing of information must be in accordance or compatible with for the purpose for which it was initially collected for.

To determine compatibility, the responsible party must take the following into account;

- Purpose of collection, and relation to intended further processing
- Nature of information concerned
- The possible consequences for the data subject in the event of further processing
- The manner in which the information was collected
- Contractual rights between the parties

7.5 Information Quality

The responsible party must take reasonable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary

7.6 Openness

Documentation of all processing operations must be maintained, in relation to the Promotion to Access of Personal Information Act (PAIA).

When personal information is collected the responsible party needs to take reasonable steps to ensure that the data subject is aware;

- Which information is collected, and where the information is not collected from the data subject, the source where it is collected from
- Name and address of the responsible party
- The purpose of information collection
- Whether or not the supply of information of that data subject is voluntary or mandatory
- Consequence of failure to provide information
- Any particular law authorising or requiring collection of the information
- Intend, if any, to transfer information internationally

7.7 Security Safeguards

A responsible party must secure the integrity and confidentiality of personal information, by implementing measures to prevent loss of, damage to, or unauthorised destruction of personal information, in addition to the restricted access of unlawful access to, or processing of personal information.

Information processed by an operator or person acting under authority:

Anyone who process information on behalf of the responsible party, must;

- Process such information only with the knowledge and authorisation of the responsible party
- Not disclose personal information, unless required to do so by law, or in the proper performance of their duties
- An operator must notify the responsible party if there is reason to believe that personal information on a data subject has been accessed or acquired by an unauthorised person

7.8 Data Subject Participation

A data Subject, having provided adequate proof of identification, has the right to;

- Confirm whether the responsible party holds any personal information on him/her, free of charge

- Request a record or description of what personal information is held by the responsible party, as well as identification on third parties who has had access to data subject personal information, at a possible prescribed fee
- The responsible party may refuse access to personal information, in part or total, on reasonable grounds as elaborated in the Promotion of Access to Information Act

Correction of personal information:

A data subject may, in a prescribed manner, request the responsible party to;

- Correct or delete personal information about the data subject in its possession, or under its control, that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully
- Destroy or delete personal information on the data subject that the responsible party is no longer authorised to retain

8 COMPANY COMPLIANCE IN REGARD TO CONDITIONS OF LAWFUL PROCESSING OF PERSONAL INFORMATION

(to be read in conjunction with 7, as above, since below stipulations can be considered additional measures, or, and measures implemented condition-specific, by the Company)

Below relays summarised detail on Nursetec's strategy in complying to the eight processing conditions as outlined by the Protection of Personal Information Act.

8.1 Accountability

Each data handler, Company Client, Company Service Provider, or Operator, will be held liable for the compliance to the conditions of lawful processing, as set forth in the Protection of Personal Information, as well as Company Policies and Procedures, relating hereto, and the Act itself, which is made available to each Employee through Company resources

8.2 Limits to Processing personal information

Nursetec will collect and process personal information of a data subject, for one of the following reasons:

- For Employee Representation, either within the Company internal framework, or with Company Clients
- To secure placement opportunities
- For Employee development purposes, including succession planning
- In addressing any internal relation matters
- To third parties, acting under Companies authority, in the event of Company representation
- To Public Bodies in the event of Company Compliance and Business requirements
- In instances were either the Protection of Personal Information, or the Promotion of Access to Information Act requires the Company to do so
- Reasons governed through other legislation

Detail specification, per category, can be referenced in Nursetec's latest PAIA Manual

8.3 Purpose Specification

The purpose as to why personal information is collected from the data subject, will be pre-eminent at the time of collection.

A data subject will be made aware of reason for collection by;

- Contractual agreement
- Obvious relation as to why personal information is collected

Retention of records, in excess than of the purpose of collection and processing:

Records will be retained for longer timeframes, in cases where Nursetec is;

- Legally required to do so
- As statutory Company compliance
- It is a contractual requirement to retain the record for a certain amount of time
- Written consent is obtained from the data subject
- For historical, statistical, or research purposes

8.4 Further processing Limitation

No personal information may be further processed, other than the intent, that what was relayed to the data subject, at the date of personal information collection.

Reasons for further processing of personal information, may include those which were categorised in the Companies PAIA Manual, under 10.2

8.5 Information quality

Personal information may only be collected from the data subject, and collection method needs to be done in writing.

A data subject is responsible to inform the Company, in the event that there were any changes to their personal information. Changes in personal information will only be done, if received in the prescribed manner, with the required supporting documentation annexed.

Data subject needs to complete **DOC NR: POL- COM – 005 – B** and return a signed copy thereof to Nursetec. No changes will be brought about, if the authenticity of the completed form, or of any of the supporting documentation cannot be verified.

8.6 Openness

Documents containing personal information, which is stored by the Company, include those listed under 10.2 of the Company PAIA Manual.

All processing information will be stored according to region, whether it be electronically or as a hard copy. Placement Personnel can expect their record to be stored at their regional reporting office, whilst permanent personnel, Company Service Providers, and Company Clients can expect their personal information to be stored at the Company Head Office. Details of irrespective offices nationwide, can be referenced in the Companies' PAIA Manual, under section 5.

8.7 Security Safeguards

Nursetec has done a strategic risk assessment with national offices (*DOC NR: POL- COM - 005 - A*), to identify personal information that can be accessed in that office, the different access levels, possible risks involved, and have given Deputy Information Officers, as well as other relational internal departments, the opportunity to make suggestions on what could be appropriate measures to implement, in order to mitigate possible risks.

Feedback on office risk assessment were reviewed and processed accordingly.

Below are some of the implemented Company security safeguards:

- Software data gets protected 24/7 through anti-virus and anti-malware programs(s). These program(s) detects threats proactively, take real-time action against cyberthreats before it takes hold, and neutralise identified threats
- The Nursetec Management Payroll System, which contains a great deal of personal information on placement personnel, is secured through restricted access. A data handler can only access this system through their unique username and password. Furthermore, all data handlers are grouped, which will determine the level of access to personal information the handler has. Each data handler only has access to information needed to perform daily operational requirements
- All functions performed, on the Nursetec Management Payroll System, can be traced
- Company utilises Cloud storage for all electronic records. Before mentioned storage is categorised according to department, whilst access are given individually to data handlers, based on records the data handler may access
- All electronic records gets backed-up offsite, where the Company Service Provider has their own anti-virus and anti-malware protection in place. In the event where there is a loss of data, data can be recovered
- Records containing personal information, of which a hard copy exists, is kept in locked storage spaces

In the event of a suspected breach the following will be executed:

- The Company Incident Management Register needs to be completed, and send to the Information Officer
- After the Information Officer have confirmed the breach to likely be true, the Information Officer will notify the Information Regulator
- Compromised data subject, whose identity can be verified, will be notified of breach. Before mentioned notification will be communicated to the data subject to his/her last known email address. In the absence

of an email address written communication will be sent to the data subjects' last known residential, or postal address

- Such a notification will include; the possible consequences of the security compromise, what the Company intends to do about the security compromise, recommendations on what the data subject needs to do to mitigate effects the security compromise may have, on the data subject, and the possible identity of the party who gained unauthorised access to personal information
- Notification of security compromise, to the data subject, will be done as soon as reasonably possible, unless otherwise prescribed by the Information Regulator

8.8 Data subject participation

A data subject is allowed to the detail surrounding personal information, that the Company has on that data subject.

Before such information may be released to alleged data subject, identity of the requestor needs to be established, prior to release. Identity will be established through a series of security questions.

Security questions will be based on information available on the data subjects' profile, as this information is classified as "last know."

A data subject has the right to request that the Company correct, delete or destroy personal information, on the data subject, for reasons listed under 7.8. When such a request is made, a data subject has to complete and return Company prescribed template (*DOC NR: POL– COM– 005 – B*), for review. A data handler will process the request accordingly, and outcome will be communicated to the data subject – if request was successfully processed, the data subject will be furnished with proof, should data subject feel it necessary, whereas if a request was denied, for whatever the reason may be, data subject will be provided with reason(s) for this decision.

9 PROCESSING OF SPECIAL PERSONAL INFORMATION

Prohibition on processing of special personal information:

A responsible party may not, subject to 9.1, process personal information concerning;

- the 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 behavior of a data subject to the extent that such information relates to, the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

9.1 The prohibition on processing personal information, as referred to above does not apply if the;

- processing is carried out with the consent of a data subject
- processing is necessary for the establishment, exercise or defence of a right or obligation in law
- processing is necessary to comply with an obligation of international public law
- processing is for historical, statistical or research purposes to the extent that, the purpose serves a public

interest and the processing is necessary for the purpose concerned, or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject

- Under the authority, or with instruction from the Regulator, to process special personal information
- 9.1 should be read together with authorisation applied to different categories of special information, in addition to the prohibition placed on the processing of personal information, relayed in, section 27 to 33, of the Protection of Personal Information Act

9.2 Criminal Checks performed by the Company

Nursetec will perform Criminal Checks on all prospective Employees, as well as existing Employees, as and when the need requires, for one, or more of the following reasons:

- Prior to possible employment opportunit(ies)
- In the event that a Company Client, prospective Client, or the Company require a criminal check be done on the data subject prior to placement, or during the course of placement period
- At any time, when an Employee takes on, or are assigned with occupational duties, of which a criminal check is a pre-requisite

When a criminal check is performed on a data subject, the data subject needs to sign both the, applicable consent of the operator, as well as the Company developed, Criminal Check Release disclaimer (*DOC NR: GEN- COM – 002*)

9.3 Processing of Other Special Personal Information

In addition to personal information relayed under 9.2, the Company may also collect, process, further process and retain below, on a data subject:

- Race
- Nationality
- Health

10 EXEMPTION ON THE PROCESSING OF PERSONAL INFORMATION

The processing of personal information will not constitute a breach if;

- Regulator grants an exemption due to public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing. The Regulator may also grant exemption if, the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing
- Exemption is granted in respect of certain function, which may include, a function performed by a public body, a function of law to protect members of the public, or in the event of unfitness or incompetence

11 RIGHTS OF DATA SUBJECTS REGARDING DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATIONS, DIRECTORIES AND AUTOMATED DECISION MAKING

The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject;

- has given his or her consent to the processing; or
- is a customer of the responsible party.

A responsible party may approach a data subject;

- whose consent is required in terms of subsection
- who has not previously withheld such consent, only once, in order to request the consent of that data subject.

12 ACCESS TO INFORMATION THROUGH PAIA

PAIA allows a requester to get access to Records, through a formal request procedure. Please see Company PAIA Manual (*DOC NR:GEN – COM – 008*) and PAIA guide to making such an application, both which are available on the Company website, on applicable Process.

A requestor can either be an individual, or a Company.

13 ENFORCEMENT

Interference with protection of personal information of data subject:

Interference with the protection of the personal information of a data subject consists of;

- any breach of the conditions as set forth under 7, 8 and 9, of this policy, as well as Chapter 3 of the Protection of Personal Information Act
- non-compliance with notification prescription in the event of a suspected compromise
- a breach of the provisions of a code of conduct issued by the Regulator

Complaints:

- Any person may submit a complaint to the Information Regulator, alleging non-compliance to the protection of personal information, of a data subject
- A responsible party, or a data subject may submit a complaint to the Regulator if he/she is aggrieved by the determination of the adjudicator
- Complaints has to be addressed to the Regulator in the prescribed manner

Modes of complaints to the Regulator:

- A complaint to the Regulator must be made in writing.
- The Regulator must give complainant assistance necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing.

13.1 Information Regulator Contact Details

The Information Regulator of South Africa, can be located at below address:

**JD House
27 Stiemens Street
Braamfontein, Johannesburg
2001**

In the event that a data subject feels that the responsible party does not Comply with Provision on the Protection of Personal Information, he or she may send an email to;

- POPIAComplaints@inforegulator.org.za

For general enquiries addressed to the Information Regulator;

- [*enquiries@inforegulator.org.za*](mailto:enquiries@inforegulator.org.za)

Action on Receipt of Compliant

On receiving a complaint, the Regulator may;

- conduct a pre-investigation as referred to below, *Pre-investigation proceedings of Regulator*
- act, at any time during the investigation and where appropriate, as conciliator in relation to any interference with the protection of the personal information of a data subject, in the prescribed manner
- decide to take no action on the complaint, or as the case may be, require no further action in respect of the complaint; conduct a full investigation of the complaint; refer the complaint to the Enforcement Committee; or take such further action as is contemplated in Chapter 10 of the Protection of Personal Information Act
- The Regulator must, as soon as is reasonably practicable, advise the complainant, and the responsible party to whom the complaint relates of the course of action that the Regulator proposes to adopt
- The Regulator may, on its own initiative, commence an investigation into the interference with the protection of the personal information of a data subject

Regulator may decide to take no action on complaint

The Regulator, after investigating a complaint received, may decide to take no action or, as the case may be, require no further action in respect of the complaint if, in the Regulator's opinion that;

- the length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable

- the subject matter of the complaint is trivial
- the complaint is frivolous or vexatious or is not made in good faith
- the complainant does not desire that action be taken
- the complainant does not have a sufficient personal interest in the subject matter of the complaint
- in cases where the complaint relates to a matter in respect of which a code of conduct is in force and the code of conduct makes provision for a complainant's procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.
- the Regulator may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Regulator that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.
- In any case where the Regulator decides to take no action, or no further action, on a complaint, the Regulator must inform the complainant of that decision and the reasons for it.

Referral of complaint to regulatory body

- If, on receiving a complaint, the Regulator considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body established in terms of any law, the Regulator must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned
- If the Regulator determines that the complaint should be dealt with by another body, the Regulator must forthwith refer the complaint to that body to be dealt with accordingly and must notify the complainant of the referral

Pre-investigation proceedings of Regulator

Before proceeding to investigate any matter, the Regulator must, in the prescribed manner, inform;

- the complainant, the data subject to whom the investigation relates (if not the complainant) and any person alleged to be aggrieved (if not the complainant), of the Regulator's intention to conduct the investigation;
- and the responsible party to whom the investigation relates of the; details of the complaint or, the subject matter of the investigation; as well as the right of that responsible party to submit to the Regulator, within a reasonable period, a written response in relation to the complaint or, the subject-matter of the investigation.

Settlement of complaints

If it appears from a complaint, or any written response made on behalf of a data subject;

- a settlement between any of the parties concerned; and
- if appropriate, a satisfactory assurance against the repetition of that action that or the doing of further actions of similar nature by the person concerned, the Regulator may, without investigating the complaint or, as the case may be, investigating the complaint further, in the prescribed manner, use its best endeavours to secure such a settlement and assurance.

Investigation proceedings of Regulator

The Regulator may;

- summon and enforce the appearance of persons before the Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court
- administer oaths
- receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Regulator sees fit, whether or not it is, or would be admissible in a court of law
- at any reasonable time, enter and search any premises occupied by a responsible party
- conduct a private interview with any person in any premises entered
- otherwise carry out in those premises any inquiries that the Regulator sees fit

Warrants, including the issuing, execution, objection and return of warrants

- to reference the Authority that the High Court has in terms of warrants, and the responsible parties rights to object, please refer to the Protection of Personal Information Act Section 82, to Section 88. For ease of reference before mentioned sections has been captioned from the Act, and added to this policy (*DOC NR: POL-COM-005-D*).

Assessment

- The Regulator, on its own initiative, or at the request by or on behalf of the responsible party, data subject or any other person must make an assessment of whether an instance of processing of personal information complies with the provisions set in the Protection of Personal Information Act

14 INFORMATION AND DEPUTY INFORMATION OFFICER(S)

The CEO of Nursetec, at any given timeframe, will fill the role of Information Officer. The Information officer will delegate responsibility to Deputy Information Officer(s), which will comprise of the Manager of each individual branch.

The Information Officer, and Deputy Information Officers, will be duly registered with the Information regulator, and information of both categories will be updated, as needed or on an Annual basis, whichever comes first.

The Information Officer reserves the right to change/revise responsibilities delegated to Deputy Information Officer(s), in writing.

15 IRRESPECTIVE DUTIES OF THE INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER(S)

15.1 Duties of The Information Officer

- The encouragement of compliance by the Body with the conditions for the lawful processing of personal information
- Dealing with requests made to the Body pursuant to POPIA
- Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA in relation to the body
- Otherwise ensuring compliance by a body with the provisions of POPIA.

15.2 Duties of Deputy Information Officer(s)

- To perform Duties/Responsibilities as assigned by the Information Officer
- Ensure Compliance to Company POPIA Policy and Procedure
- Be accessible to everyone, particularly to a data subject in respect of POPIA or a requester, in terms of PAIA
- Have reasonable understanding of POPIA, as well as PAIA
- To report all irregularities, or suspected irregularities, or any contradictions to that are prescribed in this Policy, as well as the Protection of Personal Information Act

16 PANALTIES AND FINES

Any data handler, Company Client, Company Service Provider, or Operator, who is in contravention of the Protection of Personal Information Act, will be held liable in their own capacity. Should the Company suffer any losses as a result of contravention, a Civil process will be followed, to ensure recovery from the responsible party.

A guilty party will be subject to penalty or fee, or both, as determined by the Information Regulation, or the relevant body, who shares jurisdiction, or has sole jurisdiction, over the applicable contravention

