NITO ENERGY (PTY) LTD

Protection of Personal Information Manual

Policies and Procedures

Version 2020.01

Contents

Preface

The Protection of Personal Information Act, 4 of 2013, recognizes that, in terms of the Constitution of South Africa, everyone has the right to privacy. This includes the right against unlawful collection, retention, dissemination and use of personal information. The Act therefore regulates the processing of personal information by public and private bodies in a manner that gives effect to the constitutional right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests, particularly the of access to information.

The Act requires responsible parties to take actions to ensure protection of personal information when processing, and compliance with the eight lawful conditions of processing.

Entities that make use of these resources for POPI compliance are urged to read through it carefully, consider the specific POPI implications for them and incorporate that into the manual and annexures.

Guidance have been provided in comment fields that may be deleted once the necessary edits have been performed. Fields that require editing have also been indicated in yellow or by way of a drop-down box. Please read through the manual carefully and edit where necessary.

Please note that no part of this manual or toolkit replace the responsibility of the information officer to ensure compliance, nor can it be seen, on its own, as sufficient information to provide knowledge regarding the POPI and PAIA Act to the extent required by the Information Officer and the Deputy Information Officer. Training, research and/or consultation should still be considered.

Disclaimer:

This manual is prepared by JZA Advisory and Tax (Pty) Ltd from the legislation as promulgated. JZA Advisory and Tax (Pty) Ltd assumes no liability or guarantee whatsoever for damages of any type, including and without limitation for direct, special, indirect, or consequential damages associated with the use of this manual. This manual does not constitute legal advice. Users of this manual are advised to obtain their legal advice before applying the content of this manual.

Definitions

The following terms used in this manual and legislation are defined as follows:

"The Act": The Protection of Personal Information Act, 4 of 2013, and includes any regulation under this act.

''Automated means": any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

"Biometrics": A technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

"Body": public or private body.

"Child": A natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

"Code of conduct": A code of conduct issued by the Regulator in terms of Chapter 7 of the Act.

"Competent person": Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

"Consent": Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

"Constitution": The Constitution of the Republic of South Africa, 1996.

"Data subject": The person to whom personal information relates.

"De-identify": In relation to personal information of a data subject, means to delete any information that identifies the data subject, can be used or manipulated by a reasonably foreseeable method to identify the data subject, or can be linked by a reasonably foreseeable method to other information that identifies the data subject.

"Direct marketing": To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject, or requesting the data subject to make a donation of any kind for any reason.

"Electronic communication": Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

"Enforcement notice": A notice issued by the Regulator to a responsible party in order to take certain action.

"Filing system": Any structured set of information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

"Head": of, or in relation to, a private body means:

a) in the case of a natural person, that natural person or any person duly authorised by that natural person;

b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
c) in the case of a juristic person the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer;

"Information matching programme": The comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject.

"Minister": The Cabinet member responsible for the administration of justice.

"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. This means that the information you process is not for your direct client, employee, supplier, etc. but rather that of another entity. For example, if you provide payroll services and as such process the information of another entity's employees.

"Person": A natural person or a juristic person.

"Personal information": Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

a) 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;
b) information relating to the education or the medical, financial, criminal or employment history of the person;
c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
d) the biometric information of the person;
e) the personal opinions, views or preferences of the person;
f) 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;
g) the views or opinions of another individual about the person; and
h) 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.

"POPI": Protection of Personal Information.

"POPIA": Protection of Personal Information Act

"PAIA": Promotion of Access to Information Act

"Prescribed": Prescribed by regulation or by a code of conduct.

"Private body":

a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
b) a partnership which carries or has carried on any trade, business or profession; or

c) any former or existing juristic person but excludes a public body.

"Processing": Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
b) dissemination by means of transmission, distribution or making available in any other form; or
c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

"Professional legal adviser": Any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice.

"Public body":

a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
b) any other functionary or institution when:
    a. exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
    b. exercising a public power or performing a public function in terms of any legislation.

"Public record": A record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

"Record": Any recorded information:

a) regardless of form or medium, including any of the following:
    a. Writing on any material;
    b. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
    c. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    d. book, map, plan, graph or drawing;
    e. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
b) in the possession or under the control of a responsible party;
c) whether or not it was created by a responsible party; and
d) regardless of when it came into existence.

"Regulator": The Information Regulator established in terms of section 39 of the Act.

"Re-identify": In relation to personal information of a data subject, means to resurrect any information that has been de-identified, that:

a) identifies the data subject;
b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, ''re-identified'' has a corresponding meaning.

"Republic": The Republic of South Africa.

"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.

"Restriction": To withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

"Special personal information":

a) 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
b) the criminal behaviour of a data subject to the extent that such information relates to:
    a. the alleged commission by a data subject of any offence; or
    b. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

"Unique identifier": Any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

Introduction

Lawful processing of Personal Information

Personal information may be processed if it is done in accordance with the Act and the responsible party adheres to the conditions for the lawful processing of personal information:

a) Accountability – Refer to Part 1: The Information Officer;
b) Processing limitation – Refer to Part 3: Processing Personal Information;
c) Purpose specification – Refer to Part 3: Processing Personal Information;
d) Further processing limitation – Refer to Part 3: Processing Personal Information;
e) Information quality – Refer to Part 3: Processing Personal Information and Part 4: Data subject participation;
f) Openness – Refer to part 4: Data subject participation;
g) Security safeguards – Refer to Part 5: Safeguarding of Information and Part 6: Breaches;
h) Data subject participation – Refer to part 4: Data subject participation.

The processing of special personal information is prohibited unless:

a) Consent is obtained from the Data subject;
b) processing is necessary for the establishment, exercise or defense of a right or obligation in law;
c) processing is necessary to comply with an obligation of international public law;
d) processing is for historical, statistical or research purposes to the extent that:
    a. the purpose serves a public interest, and the processing is necessary for the purpose concerned; or
    b. 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 to a disproportionate extent;
e) information has deliberately been made public by the data subject;
f) Processing is authorised by Regulator;
g) In the event of religious or philosophical belief, processing is carried out by the spiritual or religious organisation to which the data subject belongs or to which their family members belong;
h) In the event of race or ethnic origin, processing is carried out to identify data subjects or comply with specific legislation;
i) In the event of trade union membership, processing is carried out by the trade union to which the data subject belongs;
j) In the event of political persuasion, processing is carried out by or for an institution, founded on political principles if the information is of their members or employees;
k) In the event of political persuasion, processing is carried out by or for an institution, founded on political principles if the information is for the purposes of:
    a. Forming a political party;
    b. participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party;
    c. campaigning for a political party or cause.
l) In the event of health or sex life, processing is carried out by:
    a. medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject;

b. insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations;
c. schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
d. any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
e. any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures;
f. administrative bodies, pension funds, employers or institutions working for them.

m) In the event of criminal behaviour or biometric information, processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law;
n) In the event of criminal behaviour or biometric information, the processing is carried out by the employer in accordance with the rules established in compliance with labour legislation.

The processing of personal information of children are prohibited unless it is:

a) Carried out with the prior consent of a competent person;
b) Necessary for the establishment, exercise or defense of a right or obligation in law;
c) Necessary to comply with an obligation of international public law;
d) For historical, statistical or research purposes to the extent that:
    a. the purpose serves a public interest, and the processing is necessary for the purpose concerned; or
    b. 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 child to a disproportionate extent;
e) Of personal information which has deliberately been made public by the child with the consent of a competent person;
f) Processing is authorised by Regulator.

Exclusions

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

a) in the course of a purely personal or household activity;
b) that has been de-identified to the extent that it cannot be re-identified again;
c) solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.

The processing of the above information will therefore not be dealt with in this manual.

Exemptions

The regulator may grant exemption, however, at the time this manual was published there was no exemptions granted by the regulator.

Rights of Data Subjects

Data subjects have the following rights in terms of the Act:

a) to be notified that personal information is being collected or personal information has been accessed or acquired by an unauthorised person;

b) to establish whether a responsible party holds personal information of that data subject and to request access to such personal information;
c) to request, where necessary, the correction, destruction or deletion of personal information;
d) to object, on reasonable grounds relating to the particular situation, to the processing personal information;
e) to object to the processing of personal information at any time for purposes of direct marketing;
f) not to have personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as allowed – Refer to Part 7: Direct Marketing;
g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person;
h) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator;
i) to institute civil proceedings regarding the alleged interference with the protection of personal information;

Part 1: The Information Officer

Condition 1 - Accountability

As a responsible party, NITO ENERGY (PTY) LTD must ensure that the conditions for the lawful processing of personal information is complied with. This is done through the appointment of an information officer who will take responsibility and accountability for the provisions of the Act.

Information officer

NITO ENERGY (PTY) LTD is a Private body and as such our information officer is the CEO or equivalent of the entity. This individual has accepted and acknowledged their role in this capacity and is aware of the accountability that comes with it. Please refer to **Annexure 1 – Information officer** for the acceptance of this responsibility by the relevant individual.

Deputy information officer

Information Officers are required to designate one or more Deputy Information Officers. As such, NITO ENERGY (PTY) LTD has appointed a deputy information officer to whom the responsibilities in terms of the Act as well as the Promotion of Access to Information Act, will be delegated. The Deputy Information Officer will be afforded sufficient time, adequate resources and the financial means to devote to matters concerning POPIA and PAIA.

The Deputy Information Officer will report to the CEO or equivalent as Information officer. He/she will be accessible to all relevant parties within the entity as well as outside to be able to fulfill the duties. This individual will be responsible for implementing the POPI policies and procedures within the entity as set out in **Annexure 1 – Information officer.**

Despite the above-mentioned designation of a Deputy Information Officer(s), an Information Officer retains the accountability and responsibility for the functions delegated to the Deputy Information Officer.

Annexure 1 – Information officer, sets out the responsibility and accountability of the Information Officer and the Deputy Information officer, as well as the formal acceptance of these.

Registration of Information Officer

Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator. The Information Officer must complete and submit the registration form to the regulator. The current Information officer has been registered. Should there be a change in Information officer, the particulars will be updated. The Information Officer and Deputy Information Officer acknowledges that the Regulator will make their contact details available on its website.

Annexure 2 – Information Officer's registration form

Part 2: Personal Information Impact Assessment

It is the responsibility of the information officer to perform a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

This assessment should identify which parts of the Act is applicable to the entity, who are the data subjects of the entity, what information is collected and processed and what measures needs to be taken to ensure lawful processing and safeguarding of the information.

You may need to have a meeting with individuals within the company who are responsible for processing information, to be able to identify all the necessary information. **Annexure 3 - Personal information Impact assessment** will guide you through this process. This document is the foundation of your POPI manual and policies and procedures. Please make sure that it is completed correctly. Please note that this assessment and the manual interacts with one another and must be completed together. Where necessary, the manual provides further guidance as to what should be done in the impact assessment.

Data Subjects

When identifying and documenting data subjects, try and group them per Data Process, as different information may be processed for the same individual in different processes. For example, employing individuals may be one process, and completion of COVID registers may be a different process, even though the same information is collected and processed. This is due to the fact that the information is collected, used and stored in a different way, and as such needs to be evaluated and treated separately.

The following data subjects have been identified during the impact assessment for whom the processes will be implemented as per Part 3: Processing Personal Information:

a) Employees
b) Customers
c) Suppliers
d) Shareholders
e) Directors

Processing of special personal information

We process special personal information for the following data subjects:

Data subject	Reason for processing
Employees	in order to process payroll, insurance policies
Customer	To be able to provide services
Supplier	To be able to obtain services
Shareholders	To have updated share certificates
Directors	To stay updated on statutory documents

We will only process this information if one of the following is applicable:

a) Consent is obtained from the Data subject;
b) processing is necessary for the establishment, exercise or defense of a right or obligation in law;
c) processing is necessary to comply with an obligation of international public law;

d) processing is for historical, statistical or research purposes to the extent that:
    a. the purpose serves a public interest and the processing is necessary for the purpose concerned; or
    b. 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 to a disproportionate extent;
e) information has deliberately been made public by the data subject;
f) Processing is authorised by Regulator;
g) In the event of religious or philosophical belief, processing is carried out by the spiritual or religious organisation to which the data subject belongs or to which their family members belong;
h) In the event of race or ethnic origin, processing is carried out to identify data subjects or comply with specific legislation;
i) In the event of trade union membership, processing is carried out by the trade union to which the data subject belongs;
j) In the event of political persuasion, processing is carried out by or for an institution, founded on political principles if the information is of their members or employees;
k) In the event of political persuasion, processing is carried out by or for an institution, founded on political principles if the information is for the purposes of:
    a. Forming a political party;
    b. participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party;
    c. campaigning for a political party or cause.
l) In the event of health or sex life, processing is carried out by:
    d. medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject;
    e. insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations;
    f. schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
    g. any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
    h. any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures;
    i. administrative bodies, pension funds, employers or institutions working for them.
m) In the event of criminal behaviour or biometric information, processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law;
n) In the event of criminal behaviour or biometric information, the processing is carried out by the employer in accordance with the rules established in compliance with labour legislation.

This is documented in **Annexure 3 - Personal information Impact assessment**, on each relevant data subject tab.

Processing of information of children:

We do not process personal information of children:

Prior authorisation

The responsible party must obtain prior authorisation from the Regulator prior to any processing if that responsible party plans to:

a) process any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the information together with information processed by other responsible parties;
b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
c) process information for the purposes of credit reporting;
d) transfer special personal information, or the personal information of children, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

A responsible party must obtain prior authorisation only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised. This authorisation will be obtained by notifying the Regulator of the processing as above.

Responsible parties may not carry out information processing that has been notified to the Regulator until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted. The Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation. On conclusion of the more detailed investigation the Regulator must issue a statement concerning the lawfulness of the information processing. If the Responsible party does not receive the Regulator's decision within the time limits specified, it may presume a decision in its favour and continue with its processing.

At the time that this manual was published, the regulator has not yet declared the manner for providing this notification.

NITO ENERGY (PTY) LTD does not process information as above and as such does not need prior authorisation.

Part 3: Processing Personal Information

Lawfulness of processing

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject. NITO ENERGY (PTY) LTD therefore implements the below policies and procedures on the personal information processed of all data subjects identified during the Personal Information Impact Assessment as per Part 2.

Condition 2 – Processing Limitation

A responsible party will ensure that it only process data that it actually needs for the purposes of running the business, executing its contracts and protecting its legitimate interests.

Minimality

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive. As per **Annexure 3 – Personal Information Impact Assessment**, all personal information obtained per data subject will be evaluated against the purpose for processing to identify if it is adequate, relevant and not excessive. If it does not comply, it will not be processed.

Collection of data

NITO ENERGY (PTY) LTD will always aim to collect data directly from a data subject. In the following instances it is not required by the Act to receive it directly from the data subject and as such will not be a contravention:

a) The information is contained in or derived from a public record or has deliberately been made public by the data subject;
b) The data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;
c) Collection of the information from another source would not prejudice a legitimate interest of the data subject;
d) Collection of the information from another source is necessary:
    a. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
    b. 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 Service Act, 1997 (Act 34 of 1997);
    c. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
    d. In the interests of national security; or
    e. To maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;
e) Compliance would prejudice a lawful purpose of the collection; or
f) Compliance is not reasonably practicable in the circumstances of the particular case.

The source of the data is indicated on **Annexure 3 – Personal Information Impact Assessment**, per data subject.

Consent, justification and objection

NITO ENERGY (PTY) LTD will only process personal information in terms of our personal information impact assessment, if any of the following applies:

a) The data subject or a competent person where the data subject is a child consents to the processing;
b) Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
c) Processing complies with an obligation imposed by law on the responsible party;
d) Processing protects a legitimate interest of the data subject;
e) Processing is necessary for the proper performance of a public law duty by a public body; or
f) Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Special personal information and information regarding children will only be processed if consent has been received or for one of the reasons as set out in the Act as well as in this manual under the section: Lawful processing of Personal Information.

In terms of the Act, NITO ENERGY (PTY) LTD bears the burden of proof for the data subject's or competent person's consent as referred to above. The way in which consent was received, if relevant, or the reason why consent is not necessary, is documented on **Annexure 3 – Personal Information Impact Assessment**, per data subject.

The data subject or competent person may withdraw his, her or its consent, or object to the processing of personal information, at any time. We inform the data subject about this right on the documents as indicated on **Annexure 3 – Personal information Impact Assessment**. The data subjects are also informed of the consequences should they withdraw consent, and where consent cannot be withdrawn as the personal information is required by law or for the proper execution of the contract or agreement.

Withdrawal of consent or objection to processing personal information, if not done at the inception stage of agreements or when the information is obtained, may be done on Form 1 as per the regulations. This form is recreated as **Annexure 5 - Objection to the process of information.**

Where data subjects object to the processing of personal information, and the processing is not necessary for the proper execution of a contract or not required by law, we will stop processing the data immediately.

Complete **Annexure 3 – Personal information Impact Assessment** for each data subject to indicate compliance with condition 2 – processing limitation.

Condition 3: Purpose specification

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. The purpose for all personal information received by NITO ENERGY (PTY) LTD is set out in **Annexure 3 – Personal Information Impact Assessment**.

The data subjects are informed of the purpose for processing the information when such information is received directly from them. This is done in accordance with the documents as indicated on **Annexure 3 – Personal Information Impact Assessment**. Where information is not obtained directly from the Data subject, they will be informed of the purpose for processing in the same way in which consent will be requested as above, or otherwise they will be informed as soon as practicable, as set out in **Annexure 3 – Personal Information Impact Assessment**.

The following information will also be provided to the data subject:

a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;
b) the name and address of the responsible party;
c) the purpose for which the information is being collected;
d) whether or not the supply of the information by that data subject is voluntary or mandatory;
e) the consequences of failure to provide the information;
f) any particular law authorising or requiring the collection of the information;
g) the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;
h) any further information such as the:
    a. recipient or category of recipients of the information;
    b. nature or category of the information;
    c. existence of the right of access to and the right to rectify the information collected;
    d. existence of the right to object to the processing of personal information
    e. right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

It will not be necessary to provide the information as above if:

a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;
b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;
c) non-compliance is necessary:
    a. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
    b. 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 Service Act, 1997 (Act 34 of 1997);
    c. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
    d. in the interests of national security;
d) compliance would prejudice a lawful purpose of the collection;
e) compliance is not reasonably practicable in the circumstances of the particular case; or
f) the information will:
    a. not be used in a form in which the data subject may be identified; or
    b. be used for historical, statistical or research purposes.

Data Retention

personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

a) Retention of the record is required or authorised by law;
b) The responsible party reasonably requires the record for lawful purposes related to its functions or activities;
c) Retention of the record is required by a contract between the parties thereto; or
d) The data subject or a competent person where the data subject is a child has consented to the retention of the record.

Due to the administrative difficulties of managing different retention periods, NITO ENERGY (PTY) LTD's policy is to retain all information for a maximum of five years after the conclusion of the agreement, contract or service for which it was obtained. This will allow NITO ENERGY (PTY) LTD to comply with all legislative requirements of retention. This will be communicated to data subjects as provided for in **Annexure 3 – Personal Information Impact Assessment**. Should a Data subject not consent to this, the retention period will default back to the prescribed period as per legislation. These Data subjects will be flagged to ensure that their records are destroyed after the retention period. For all other personal data, it will be destroyed after the five year retention period.

Condition 4: Further processing limitation

Further processing refers to any processing of personal information for reasons other than those for which it was obtained and that have already been communicated to the data subject.

NITO ENERGY (PTY) LTD will only process information further if it is in accordance or compatible with the purpose for which it was collected. To assess whether further processing is compatible with the purpose of collection we will take the following into account:

a) The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

b) The nature of the information concerned;
c) The consequences of the intended further processing for the data subject;
d) The manner in which the information has been collected; and
e) Any contractual rights and obligations between the parties.

Information may be processed further without performing the above considerations if:

a) The data subject or a competent person where the data subject is a child has consented to the further processing of the information;
b) The information is available in or derived from a public record or has deliberately been made public by the data subject;
c) Further processing is necessary:
    a. to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
    b. 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 Service Act, 1997 (Act 34 of 1997);
    c. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
    d. in the interests of national security;
d) The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:
    a. public health or public safety; or
    b. the life or health of the data subject or another individual;
e) The information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
f) The further processing of the information is in accordance with an exemption granted.

The above considerations will be made every time information is subjected to further processing and documented per class of data subject for which further processing may be necessary. See **Annexure 7 – Further processing.**

Condition 5: Information quality

A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

To ensure quality of personal information, data subjects are provided with the opportunity to contest the accuracy of the information on Form 2, see **Annexure 6 – Request for correction or deletion of personal information**. We will restrict the processing of personal information in these instances in order to verify the accuracy of the information.

On receipt of a request for correction we will, as soon as reasonably possible:

a) Correct the information or destroy or delete the information, depending on the relevant request;
b) Provide the data subject, to his or her satisfaction, with credible evidence in support of the information, or where agreement cannot be reached between us and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made;

c) Inform each person or body or responsible party to whom the personal information has been disclosed of these steps;
d) Inform the data subject of the result of the request.

When we become aware of information that may be incorrect, we will institute the necessary process to obtain accurate information. This process will depend on where the information is documented and stored and who is responsible for it. The process for ensuring information quality per data subject is as follows:

Data Subject	**Process**
Employees	employee information sheet completed by employee and signed
Customers	Information is providing on the enquiry and purchase orders.
Suppliers	Email or telephone call to update information
Shareholders	When purchasing share so on the transfer share document
Directors	On minutes of meeting when appointing new directors

Transborder Information Flows

NITO ENERGY (PTY) LTD does not transfer any data to a third party who is in a foreign country.

Part 4: Data Subject Participation

The data subject has the right to be aware of their personal information being processed and to take part in this process by either objecting to such processing or ensuring that the information is correct by requesting the responsible party to remove or correct incorrect information.

Condition 6: Openness

NITO ENERGY (PTY) LTD will take all reasonably practicable measures to inform data subjects about the personal information being processed and other information as documented under Condition 3: Purpose specification. This will be done as indicated in **Annexure 3 - Personal Information Impact Assessment**. Consent is given when the documents are signed by the data subject.

Any data subject may, having provided adequate proof of identity, request us to confirm whether or not we hold personal information about them and the identity of third parties who have, or have had access to the information.

This is done in terms of the Promotion of Access to Information Act on Form C. Please see **Annexure 9 – Request for access to record of a private body**.

If, in response to a request as above, personal information is communicated to a data subject, the data subject will be advised of their right to request the correction of information as per **Annexure 6 - Request for correction or deletion of personal information**.

A data subject may need to pay a fee for these services provided to the data subject to enable us to respond to a request. These fees will always be charged in terms of the Promotion of Access to information Act. See **Annexure 14 - Prescribed fees in terms of PAIA**.

Where these fees are applicable, we will give the applicant a written estimate of the fee before providing the services.

Access to information will be granted or refused, as the case may be, as requested by the Promotion of Access to Information Act, after taking into considerations all the requirements of this Act.

Part 5: Safeguarding of Information

Condition 7: Security safeguards

NITO ENERGY (PTY) LTD will 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:

a) Loss of, damage to or unauthorised destruction of personal information; and
b) Unlawful access to or processing of personal information.

NITO ENERGY (PTY) LTD has performed a risk assessment to identify internal and external risks to personal information in our possession or under our control. This was done based on where information is stored and who has access to it to identify the risk of the above.

The risks identified are as follows:

a) Loss of Data
b) Unauthorised access or theft of data
c) Unauthorised sharing of data
d) Inaccurate and outdated data
e) Employees sharing information

Safeguards have been implemented to mitigate the identified risks. These safeguards are monitored on a monthly basis and updated as necessary where deficiencies are identified.

The following safeguards are implemented:

a) Fireproof safe offsite and back up policy daily
b) Access controls such as locked cabinets offsite and Antivirus, firewalls and IT policy - suspicious links
c) Access controls and confidentiality agreements and Antivirus, firewalls and IT policy - suspicious links
d) Update policies and Access controls to premises as well as username and password for computers.
e) Only one employee has access

This is documented in **Annexure 8 – Risk assessment and safety measures**.

Making use of an operator

NITO ENERGY (PTY) LTD do not make use of operators to process personal information.

Performing services as an operator

NITO ENERGY (PTY) LTD does not perform services as an operator.

Part 6: Breaches

Notification of security compromises

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, NITO ENERGY (PTY) LTD shall notify:

a) the Regulator; and
b) the data subject, unless the identity of such data subject cannot be established.

The notification will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The notification will only be delayed if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a data subject shall be in writing and communicated to the data subject in at least one of the following ways:

a) Mailed to the data subject's last known physical or postal address;
b) sent by e-mail to the data subject's last known e-mail address;
c) placed in a prominent position on the website of the responsible party;
d) published in the news media; or
e) as may be directed by the Regulator.

The following information will be included in notifications:

a) a description of the possible consequences of the security compromise;
b) a description of the measures that we intend to take or have taken to address the security compromise;
c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
d) if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

Part 7: Direct Marketing

Processing of personal information for the purposes of direct marketing is allowed, provided that it complies with the eight conditions of lawful processing.

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:

a) has given his, her or its consent to the processing; or
b) is a customer of the responsible party and:
    a. The responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
    b. The processing is for the purpose of direct marketing of the responsible party's own similar products or services; and
    c. The data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details.

Consent

A responsible party may approach a data subject only once, and in the prescribed manner and form, for this consent. If the consent has been withheld previously, the data subject may not be approached again to request consent or to provide such direct marketing. The data subject may opt-in to the direct marketing again should they choose to.

A responsible party who wishes to process personal information of a data subject for the purpose of direct marketing by electronic communication must submit a request for written consent to that data subject in a form similar to Form 4 – See **Annexure 11 - Consent for Direct Marketing**. This consent must be positive and not an absence of objection.

Where Direct marketing is sent by electronic means, it must contain details of the identity of the sender or the person on whose behalf the communication has been sent, and an address or other contact details to which the recipient may send a request that such communications cease.

Implementation – Direct marketing by electronic means to new potential clients

NITO ENERGY (PTY) LTD does not process personal information for the purpose of direct marketing to new potential clients.

Implementation – Direct marketing by electronic means to existing clients

NITO ENERGY (PTY) LTD does not process personal information for the purpose of direct marketing to existing client.

Directories

A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included, must be informed, free of charge and before the information is included in the directory:

a) about the purpose of the directory;
b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.

A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

NITO ENERGY (PTY) LTD does not make their directories available to the public.

Part 8: Internal training and awareness

Training

Training will be provided at regular intervals to employees as well as to the Information Officer and Deputy Information Officers in order to ensure that everyone is informed and keep abreast of the requirements of POPIA and PAIA, as well as the policies and procedures within the entity to ensure compliance.

Training will be provided as follows:

1. New employees – Formal training session upon employment as part of the induction process
2. Existing employees – Internal workshops and discussions on specific requirements and responsibilities to be held on a regular basis (at least once a year) and formal training will be utilized if necessary.
3. Information officer and Deputy Information Officers – Formal training will be attended as induction for the position, and regular research will be performed by the Deputy Information Officer, who will in turn inform the Information Officer of any relevant information. Formal training will be utilized if necessary.

Part 9: Information Regulator

The Information Regulator has jurisdiction over the Act to educate, guide, monitor and enforce the Act.

Reporting to the Information regulator

The entity is required to report any breach of personal information to the Information Regulator.

Complaints

Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject.

A responsible party or data subject may submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of an adjudicator.

These complaints are to be done on form 5. **See Annexure 10 – Complaints.**

Part 10: Promotion of Access to Information Act

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

Section 51: Manual on functions of, and index of records held by, private body

The head of a private body must make a manual available containing:

a) in general:
    a. the postal and street address, phone and fax number and, if available, electronic mail address of the head of the body;
    b. such other information as may be prescribed;
b) insofar as PAIA is concerned:
    a. a description of the guide of how to use the PAIA as referred to in section 10, if available, and how to obtain access to it;
    b. the latest notice, if any, regarding the categories of records of the body which are available without a person having to request access in terms of PAIA;
    c. a description of the records of the body which are available in accordance with any other legislation;
    d. sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject;
c) insofar as the Protection of Personal Information Act, 2013, is concerned:
    a. the purpose of the processing;
    b. a description of the categories of data subjects and of the information or categories of information relating thereto;
    c. the recipients or categories of recipients to whom the personal information may be supplied;
    d. planned transborder flows of personal information; and
    e. a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

The head of a private body must on a regular basis update the manual.

The manual must be made available:

a) on the web site, if any, of the private body;
b) at the principal place of business of the private body for public inspection during normal business hours;
c) to any person upon request and upon the payment of a reasonable amount; and
d) to the Information Regulator upon request.

Part 11: Annexures

Part 12: References

- Protection of Personal Information Act 4 of 2013
- Regulations relating to the protection of personal information.
- Promotion of Access to Information Act 2 Of 2000