Protection of Personal Information

Lawnpro's Guidelines on

The Protection of Personal Information

Registration number:
2017/336969/07
Main place of business:
29 Leslie Street, Murrayfield, Pretoria

Table of contents

Introduction:

The **purpose** of this document is to provide a **guideline** on the interpretation of the important rights and obligations as stipulated in the Protection of Personal Information Act (hereafter referred to as POPI) with regard to the Business.

The purpose of this Act:

- To give effect to the constitutional **right to privacy**, in particular the safeguarding of personal information;
- Regulate the **processing** of personal information in harmony with international standards;
- Prescribe minimum **requirements** for the lawful processing of personal information;
- Provide the rights and **remedies** for the protection against abuses of personal information; and
- Establish an **Information Regulator** to promote, enforce and fulfil the rights protected by POPI.

This Act regulates the following:

- **Collection** and **procurement** of personal information;
- **Lawful** processing of personal information;
- **Retention** and **restriction** of records;
- **Security** safeguards and compromises;
- Processing of **special** personal information;
- Processing of personal information of **children**;
- Establishment of **Information Officer** and **Information Regulator**;
- Rights of data subject regarding **direct marketing**;
- **Transborder** information flow;
- Information Regulator's powers and **authorities**; and
- Fines and **penalties**.

Definitions:

In this Act –

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

"automatic calling machine": means a machine that is able to do automated calls without human intervention.

"binding corporate rules": means personal information processing policies, within a group of undertakings, which are adhered to by the business or operation within that group of undertakings when transferring personal information to a business or operator within that same group of undertakings in a foreign country.

"data subject": means the person to whom personal information relates.

"direct marketing": means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a) Promoting or offering to supply, in the ordinary course of business, any goods or service to the data subject; or

b) Requesting the data subject to make a donation of any kind for any reason.

"electronic communication": means 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.

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

"group undertakings": means a controlling undertaking and its controlled undertakings.

"information officer": of, or in relation to, a –

a) Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of this Act; or

b) Private body means the head of a private body as contemplated in Section 1, of The Promotion of Access to Information Act.

"operator": means 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.

"person": means a natural person or a juristic person.

"personal information": means 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, 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 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.

"private body": means –

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": means 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.

"Promotion of Access to Information Act": means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

"public body": means –

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 –
    I. Exercising a power or performing a duty in terms of the Constitution or a Provincial Constitution; or
    II. Exercising a public power or performing a public function in terms of any legislation.

"public record": means 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": means any recorded information –

a) Regardless of form or medium, including any of the following:

I. Writing on any material;

II. Information produced, recorded or stored by means of any recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently divided from information so produced, recorded or sorted;

III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

IV. Book, map, plan, graph, or drawing;

V. 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; and

c) Regardless of when it came into existence.

"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

"re-identified": has a corresponding meaning.
"responsible party": means 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": means 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": means personal information as referred to in Section 26 of this Act.
"terrorist and related activities": means those activities referred to in Section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.
"this Act": means the Protection of Personal Information Act, No. 4 of 2013.
"unique identifier": means 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.

Application of this Act:

1) This Act applies to the processing of personal information –

a) Entered in **a record** by or for a responsible party by making use of **automated or non-automated** means. Providing the recorded personal information is processed by non-automated means, it must form part of a filing system or is intended to form part thereof; and

b) The responsible party is –

I. Domiciled in the Republic; or

II. Not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

2) a) This Act applies, subject to paragraph (b), to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of this Act.

b) If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3 of this Act, the extensive provisions will prevail.

3) This Act applies to public and private bodies.

Exclusions of this Act:

1) This 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) By or on behalf of a public body –

I. Which involves **national security**, including activities that are aimed at assisting in the identification of the financing of terrorists and related activities, defence or public safety; or

II. 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;

d) By the **Cabinet** and its committees or the **Executive Council** of a province; or

e) Relating to the **judicial functions** of a court.

2) This Act does not apply to the processing of personal information solely for the purpose of **journalistic**, literacy 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.

3) The Regulator may grant **further exemptions** to comply with the conditions for lawful processing of personal information as stipulated in this Act.

Duties and Responsibilities of the Information Officer (Section 55 and 56)

1) The Information Officer's responsibilities include –

a) The encouragement of **compliance**, by the business, with the conditions for the **lawful processing** of personal information;

b) Dealing with **requests** made to the business pursuant to this Act;

c) Working with the Regulator in relation to **investigations** conducted pursuant to Chapter 6 of this Act in relation to the business;

d) Ensuring **compliance** by the business with the provisions of this Act.

The Regulations relating to the protection of personal information further stipulates additional roles and responsibilities of the information officer, according to section –

"***4.*** *(1) An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that-*

(a) a compliance framework is developed, implemented, monitored and maintained;
(b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
(c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
(d) internal measures are developed together with adequate systems to process requests for information or access thereto; and
(e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

(2) The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time."

2) The Information Officer must take up his/her duties in terms of this Act only after the business has **registered** him/her with the Regulator.

3) The business must make provisions, in the manner prescribed in Section 17 of the Promotion of Access to Information Act, for –

a) The appointment of such **number of persons**, if any, as **Deputy** I**nformation Officers** as is necessary to perform the duties and responsibilities of the Information Officer; and

b) Any **power or duty** conferred or imposed on the Information Officer by this Act, to be bestowed a **Deputy Information Officer(s)** of the business.

4) The Information Officer of a business will be the Chief Executive Officer, Owner or equivalent officer, or any person duly authorised by the Business.

5) **It is important to note** that the business may be charged with an administrative fine or the appropriate person may be sentenced to imprisonment in the event that a section or sections of this Act is contravened. It is therefore suggested that the business appoints a person with **authority** such as the Chief Executive Officer as the Information Officer to ensure that the sections as discussed hereafter are adhered to.

A. Conditions for Lawful Processing of Personal Information

The Information Officer must ensure that the business adheres to the following conditions for the lawful processing of personal information:

1) Accountability **(Section 8)**
2) Processing Limitation **(Section 9 – 12)**
3) Purpose Specification **(Section 13 – 14)**
4) Further Processing Limitation **(Section 15)**
5) Information Quality **(Section 16)**
6) Openness **(Section 17 – 18)**
7) Security Safeguards **(Section 19 – 22)**
8) Data Subject Participation **(Section 23 – 25)**

A.1 Condition 1 – Accountability (Section 8)

The business must ensure that the **conditions** of lawful processing of personal information and all measures that give effect to such conditions are **complied** with at all times.

1) The implication of this section is that the business remains **responsible** for the lawful processing of personal information regardless of it having passed the information on to a third party to process the personal information.

2) In order for the business to exercise **control** over the lawful processing of personal information, the following control measures need to be established and maintained:
    a) All **personal information** being processed by the business needs to be **identified**; and

    b) The **Information Officer and his/her Deputy Officer(s)** must be identified and **appointed** to ensure that all personal information being processed comply with the requirements of this Act.

A.2 Condition 2 – Processing Limitation

2.1 Lawfulness of Processing (Section 9)

Personal information must be processed in a **lawful** and **reasonable manner** that does not infringe the privacy of the data subject.

1) The business may not act **unlawfully** in its collection or processing of personal information.

2) To ensure the processing of personal information is done in a reasonable manner, the business must take into account the **interests** and **reasonable expectations** of data subjects as well as all of the **provisions** that are incorporated in these conditions.

2.2 Minimality (Section 10)

"Personal information may only be processed providing the **purpose** for which it is processed, it is **adequate**, **relevant** and **not excessive**."

1) This condition is closely linked to the **purpose** for which information may be processed. The business may only collect personal information that is appropriate for the **purpose** it is being collected for, and should therefore be adequate, relevant and not excessive.

2.3 Consent, justification and objection (Section 11)

2.3.1) The business may only process the personal information of a data subject if –

1) The data subject or a competent person where the data subject is a child **consents** to the processing;
2) The processing is **necessary** to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
3) The processing complies with an **obligation** imposed by law on the business;
4) The processing protects a **legitimate** interest of the data subject;
5) The processing is necessary for the proper performance of a **public law** duty by the business; or
6) The processing is necessary for pursuing the legitimate **interests** of the business or of a third party to whom the information is supplied;

2.3.2) a) **The business** bears the **burden of proof** to show that the data subject or competent person has consented to the processing of the personal information as referred to in paragraph 2.3.1.1.

b) The **data subject** or competent person may **withdraw** his, her or its consent, at any time provided that: the lawfulness of the processing of personal information before such

withdrawal or processing of personal information in terms of paragraph 2.3.1.2 – 2.3.1.6 will not be affected.

2.3.3) A **data subject** may **object** at any time, to the processing of personal information –

1) In terms of paragraph 2.3.1.2 – 2.3.1.6, in the prescribed manner, on **reasonable grounds** relating to his, her or its particular situation, unless legislation provides for such processing; or
2) For purposes of **direct marketing** other than direct marketing by means of unsolicited electronic communication as referred to in Section 69 of this Act.

2.3.4) If a **data subject has objected** to the processing of personal information in terms of paragraph 2.3.3, the business may **no longer** process the personal information.

Note to Information Officer:

1) It is important to understand that **consent** plays a vital role in processing personal information, but it is not the only consideration taken into account in order to comply with this Act.

2) This Act defines "consent" as meaning "**voluntary**, **specific** and **informed expression** of will in terms of which a data subject agrees to the processing of personal information relating to him or her." The consent must therefore be voluntary and not amount to a submission made by making use of physical force, coercion, undue influence, pressure, duress, harassment, unfair tactics or any similar conduct that may be unfair. This Act **does not require the consent to be in writing**, however, taking into consideration that the business bears the burden of proof that consent was given, it **would be advisable** to ensure that consent is obtained in writing.

3) It is important to note that consent relating to the use of personal information is **revocable** by a data subject at any time.

4) The provisions of paragraph 2.3.1.2 – 2.3.1.6 provides for conditions where the business may **lawfully** process personal information without the consent of the data subject.

5) A data subject may **object**, at any time, on reasonable grounds against the processing of personal information, whereafter the business must immediately **stop** processing the data subject's personal information.

2.4 Collection directly from data subject (Section 12)

As far as possible, the business should collect personal information **directly** from the data subject, except under the following circumstances:

1) The information is contained in or derived from a **public record** or has deliberately been made **public** by the data subject;

2) 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**;

3) Collection of the information from another source would not **prejudice** a legitimate **interest of the data subject**;

4) 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;
    c. For the **conduct of proceedings** in any **court** or **tribunal** that have commenced or are reasonably contemplated;
    d. In the interest of **national security**; or
    e. To maintain the l**egitimate interests** of the business or of a third party to whom the information is supplied;

5) Compliance would **prejudice** a lawful purpose of the collection; or

6) Compliance is **not reasonably practicable** in the circumstances of the particular case.

Note to Information Officer:

1) The business must collect personal information **directly** from the data subject, unless allowed for as stipulated in the exceptions.

2) If personal information is collected from a third party, the data subject should be made **aware** of the processing of the information and the **purpose** for which the information has been collected.

3) 3)This is a very **strict** requirement that is imposed by this Act, however, the **exceptions** are extensive and the impact of this provision is considerably softened by the application of the exceptions.

A3. Condition 3 - Purpose Specification

3.1 Collection for specific purpose (Section 13)

The business must adhere to the following requirements as stipulated by this Act:

1) The business may only collect personal information for a **specific**, **explicitly defined** and **lawful** purpose that relates to the function or activity of the business.

2) The business must have standard operating procedures in place to ensure that the data subject is **aware** of the purpose for which the information is collected.

Note to Information Officer:

1) The purpose of the collection and processing of personal information influences every aspect of the processing of the information which includes the manner of its collection, periods of retention, further processing, destruction of information, disclosure to third parties and any further matters which may apply to the processing of the information. It is therefore advisable that the **business** firstly determines the **purpose** of and the means for processing personal information prior to collecting the information.

2) In conjunction with Section 10 of this Act, this Section requires that the business only collect personal information that is adequate, relevant and not excessive given the purpose for which it will be used. Therefore, the business should first establish the **purpose** of collecting personal information from a data subject and then ensure that it is **relevant** and **not excessive** for the purpose that the information was collected for.

3) The business must ensure, in collecting the information, that the data subject is aware of the **purpose** for which the information is being collected. This enables the data subject to make an **informed decision** as to whether the personal information should be made available to the business. The business will be able to **comply** with this requirement by **stating the purpose** of collecting the personal information on the document or contract on which the information should be supplied.

3.2 Retention and restriction of records (Section 14)

The business must adhere to the following requirements as stipulated by this Act:

1) If the purpose for which information was collected or subsequently processed has been achieved, the business may then **not retain** that records any longer than necessary, unless–

a) Retention of the personal information record is **required** or authorised by law;

b) The business reasonably requires the personal information records for **lawful purposes** which has a direct relation to the business's functions or activities;

c) A contract between the parties requires the personal information records to be retained; or

d) The data subject or a competent person where the data subject is a child has **consented** to the retention of the record for a longer period.

2) The business must take note that records of personal information may be retained for periods in excess of those contemplated in paragraph (1) for **historical**, **statistical** or **research** purposes if the business has appropriate **safeguards** in place to prevent personal information records from being used for any other purposes.

3) If the business has used a record of personal information of a data subject to make a decision about the data subject, the business must –

a) **Retain** the personal information record for the period as prescribed by law or any other code of conduct; or

b) If there is no law or code of conduct prescribing a **retention** period, the business must retain the record for a period sufficient enough for the data subject to have a reasonable opportunity to **request** access to the record.

4) It is important to note that the business must **destroy**, **delete** or **de-identify** a record of personal information as soon as reasonably practicable after the business is no longer authorised to retain the record.

5) The destruction, deletion or de-identifying of a personal information record must be done in a manner that **prevents** its **reconstruction** in an intelligible form.

6) The business must **restrict** processing of personal information if –

a) Its **accuracy** is contested by the data subject, for a period enabling the business to verify the accuracy of the information;

b) The business **no longer needs** the personal information for achieving the **purpose** for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

c) The processing is unlawful and the data subject **opposes** its destruction or deletion and requests the restriction of its use instead; or

d) The data subject requests to transmit the personal information into another **automated processing system.**

7) Personal information referred to in paragraph (6) may, with the exception of storage, only be processed for **purposes of proof**, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

8) Where processing of personal information is restricted pursuant to paragraph (6), the business **must inform the data subject before lifting the restriction** on processing.

9) The business should ensure that all personal information retained are **identified**, **categorised** and appropriately **safeguarded**.

A4. Condition 4 – Further Processing Limitation

4.1 Further processing must be compatible with the purpose of collection

The business must adhere to the following requirements as stipulated by this Act:

1) Further processing of personal information must be done in accordance with the **purpose** for which it was originally collected.

2) **To assess whether further processing is compatible** with the purpose of collection, the business must take account of –

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 personal information has been collected from the data subject; and

e) Any **contractual rights** and **obligations** bestowed on the parties.

3) **Further processing of personal information is not incompatible** with the purpose of collection 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 –

I. To avoid **prejudice** to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

II. To comply with an **obligation** imposed by law or to enforce legislation concerning the collection of revenue;

III. For the conduct of proceedings in any **court or tribunal** that have commenced or are reasonably contemplated;

IV. In the interest of **national security.**

d) The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to –

I. **Public health** or **public safety**; or

II. The **life** or **health** of the data subject or another individual(s);

e) The information is used for **historical**, **statistical** or **research purposes** and the business ensures that the further processing is carried out solely for such purposes and will not be published in an **identifiable form**.

Note to Information Officer:

1) The personal information may only be further processed if such further processing is compatible with the **purpose** for which it was initially collected. For instance, if personal information was collected from a data subject with the purposes of concluding a credit agreement, the information may then not be further processed to contact the data subject to market any other services or products.

A5. Condition 5 – Information Quality

5.1 Quality of information (Section 16)

Note to Information Officer:

1) The business must take reasonably practicable steps to ensure that the personal information is **complete**, **accurate**, **not misleading** and **updated** where necessary.

2) It is important for the business to have consideration for the **purpose** for which personal information is collected or further processed.

3) In order for the business to ensure that the personal information is complete, accurate, not misleading and updated, it requires that the business have appropriate information security measures in place to **safeguard** the integrity of the personal information.

4) **Chapter 3 of the Electronic Communications and Transactions Act** also requires that the integrity, reliability and accuracy of electronic information be **maintained** if they are to enjoy the efficacy that the Act bestows upon them.

5) It is suggested that the business evaluates its information security measures on a regular basis to ensure that the personal information in its possession, remains accurate and relevant. It is further suggested that areas of concern must be identified and addressed to ensure that no information breaches occur.

A6. Condition 6 – Openness

6.1 Documentation (Section 17)

Note to Information Officer:

1) The business must maintain the documentation of all information processing operations within the business. This should be done in accordance with **Section 14** and **Section 51 of the Promotion of Access to Information Act**.

a) Section 14 stipulates that the Information Officer of a **public body** must compile an information manual in at **least three official languages** containing the following:

I. A description of **the business's structure** and core functions;

II. The **postal** and **street address**, phone and fax number and, if available, electronic mail address of the Information Officer and his/her Deputy Information Officer(s);

III. A **description** of the **business information guide;**

IV. Sufficient detail describing the **process to facilitate a request** for access to a record, including a description of the subjects on which the business holds records and the categories of records held on each subject;

V. The **latest notice**, if any, regarding the categories of records of the business which are available without a person having to request access in terms of this Act;

VI. A **description of the services available** to members of the public, provided by the business, and how to gain access to those services;

VII. A **description of any arrangement or provision** for a person making representations or influence the formulation of policies or exercise powers or performance of duties, by the business;

VIII. A **description of all the remedies** available in respect of an act or a failure to act by the business;

IX. Any **other information** as may be required.

b) Section 51 stipulates that the Information Officer of a **private body** must compile a manual containing the following information:

I. The postal and street address, phone and fax number and, if available, electronic mail address of the head of the business;

II. A description of the business information guide and how to gain access to that guide;

III. The latest notice, if any, regarding the categories of records of the business which are available without a person having to request access in terms of this Act;

IV. A description of the records of the business which are available in accordance with any other legislation;

V. Sufficient detail describing the process to facilitate a request for access to a record, including a description of the subjects on which the business holds records and the categories of records held on each subject;

VI. Any other information as may be required.

6.2 Notification to data subject when collecting personal information (Section 18)

Note to Information Officer:
1) It is important to note that when a business collects personal information to be processed for a specific purpose, the business must take reasonably practicable steps to ensure that the data subject is aware of –

a. The **type of personal information** being collected and where the personal information is not collected directly from the data subject, the **source** from which it is collected;
b. The **name** and **address** of the business;
c. The **purpose** for which the personal information is being collected;
d. Whether or not the supply of the personal information by that data subject is **voluntary** or **mandatory**;
e. The **consequences** of failure to provide the personal information;
f. Any particular **law** authorising or requiring the collection of the personal information;
g. Whether the business 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 –

I. **Recipient** or category of recipients of the information;

II. **Nature** or category of the information;

III. Existence of the right of **access** to and the right to **rectify** the information collected;

IV. **Existence of the right to object** of the processing of personal information; and

V. Right to lodge a **complaint** to the **Information Regulator** and the **contact details** of the Information Regulator.

2) Be advised that the business **do not** have to comply with paragraph 1 if:

a) The data subject or a competent person where the data subject is a child has provided **consent** for the non-compliance;

b) The business's non-compliance would not prejudice the **legitimate interests** of the data subject;

c) The business's non-compliance is necessary –

I. To avoid **prejudice** to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

II. To comply with an **obligation** imposed by law or to enforce legislation concerning the collection of revenue;

III. For the conduct of proceedings in any **court or tribunal** that have commenced or are reasonably contemplated;

IV. In the interest of **national security**.

d) The compliance would **prejudice** a lawful purpose of the collection of personal information;

e) The compliance is not reasonably **practicable** in certain circumstances of a particular case; or

f) The personal information will –

I. **Not be used** in a form in which the data subject may be **identified**; or

II. Be used for **historical**, **statistical** or **research purposes**.

3) It is important for the business to provide the data subject with the information as stipulated in paragraph 1, to ensure **transparency** and **fairness** in the processing of personal information. There are however **exceptions to the compliance** with paragraph 1 and this should be established prior to any information being collected from a data subject.

4) In the event that the business have previously taken steps to provide the data subject with the information as stipulated in paragraph 1, the business do not have to comply with paragraph 1 for any further processing of the personal information, providing the information is being processed for the same purpose for which it was collected.

A7. Condition 7 – Security Safeguards

7.1 Security measures on integrity and confidentiality of personal information (Section 19)

Note to Information Officer:

1) The business must secure the **integrity** and **confidentiality** of all personal information that is in its possession or under its control to prevent –

a) **The loss** of, **damage** to or **unauthorised** destruction of personal information; and

b) **The unlawful access** to or processing of personal information.

2) The business will comply with paragraph 1 if it ensures that appropriate, reasonable technical and organisational measures are in place to –

a) **Identify** and **document** all reasonably foreseeable internal and external **risks** that may have an influence on the personal information in its possession or under its control;

b) **Establish** and **maintain** appropriate **safeguards** against the risks identified;

c) **Regularly verify** and **obtain confirmation** that the safeguards are effectively implemented; and

d) Ensure that the safeguards are **continuously updated** in accordance with **newly identified risks** or deficiencies that may influence the current safeguards.

3) The business must **favourably consider** and take into account generally **accepted information security practices** and **procedures** that may be required in terms of specific industry or professional rules and regulations.

4) The business must ensure that **industry specific safety measures** pertaining to its personal information are implemented, evaluated and updated on a regular basis to counter any existing and potential threats it poses to the current safeguards.

5) It is advisable that the business conduct regular training sessions for its employees, especially employees which form part of the processing of personal information within the business.

6) In order to establish an information security system, the Information Officer must ensure that it addresses the three primary components that are present in the processing of personal information. The three components are **technology**, **process** and **people**.

7) The business must take note that even though certain functions which relates to the processing of personal information **may be outsourced** to third parties, for instance the provision of IT and communication services, the retention and back up of documents or even the storage and destruction of documents, it is ultimately the responsibility of the business to establish, maintain and review the information security systems.

8) It is important to note that in **allowing external parties access to the premises**, information systems or information, the access should be properly controlled and the external parties will be subject to the express requirements and prohibitions as stipulated in the **Access Control Policy**.

7.2 Information processed by operator or person acting under authority from the business (Section 20)

Note to Information Officer:

1) The business must ensure that an operator or anyone, including but not limited to, sub-contractors, agents, suppliers, importers, exporters, representatives, service providers or manufactures which process personal information on behalf of the business, must –

a) Process such information only with the **knowledge** or **written authorisation** of the business; and

b) Treat the personal information that comes to their knowledge as **confidential** and **must not disclose it**.

2) It is therefore suggested that the business incorporate a **standard written agreement** with an operator or anyone, including but not limited to, sub-contractors, agents, suppliers, importers, exporters, representatives, service providers or manufactures prior to any personal information being forwarded to him, her or it.

7.3 Security measures regarding information processed by operator (Section 21)

Note to Information Officer:

1) The business must in terms of a **written contract** between the operator and itself, ensure that the required security measures (as stipulated in Section 19), relevant to the processing of personal information, are clearly stipulated and agreed upon. The operator responsible for processing the personal information on behalf of the business, must ensure that it **establishes** and **maintains** the required security measures as he, she or it may also be held liable for any contravention of this Act.

2) The operator must **notify** the business **immediately** where there are reasonable grounds to believe that the personal information of a data subject has been lost, accessed or acquired by any unauthorised person or an information breach has occurred.

7.4 Notification of security compromises (Section 22)

Note to Information Officer:

1) If the business believes or has determined that the personal information of a data subject has been lost, accessed or acquired by any unauthorised person or an information breach has occurred the business must **notify** –

a) The **Regulator**; and

b) The **data subject**, unless the identity of such data subject cannot be established.

2) It is important to note that this **notification must 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 **business's information system**.

3) The business may only **delay notification** to the data subject 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.

4) The business must **notify the data subject in writing** and ensure that this communication reaches the data subject in at least one of the following ways:

a) **Mailed** to the data subject's last know 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 business;

d) **Published** in the news media; or

e) As may be **directed by the Regulator**.

5) The business must ensure that the written notification **provide sufficient information** to allow the data subject to take **protective measures** against the potential consequences of the compromise, including –

a) A **description** of the possible **consequences** of the security compromise;

b) A **description** of the **measures** that the business intends to take or has 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 know to the business, **the identity** of the **unauthorised person** who may have accessed or acquired the personal information.

6) The business must take note that the Regulator may direct him, her or it to **publicise**, in any manner specified by the Regulator, the fact of any compromise to the **integrity** or **confidentiality** of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise. Should it be required from the business to publish a notification, it must be taken into account that the **business's reputation** is at risk and great consideration should be given to the wording of the notification.

7) It is suggested that the business implement adequate **policies** and **procedures** that govern the notification and reporting of a compromise of personal information.

A8. Condition 8 – Data subject's participation

8.1 Access to personal information (Section 23)

Note to Information Officer:

1) Should a data subject provide adequate and/or sufficient proof of identity the data subject has the right to –

a) Request the business to **confirm**, free of charge, whether or not the business holds personal information about him, her or it; and

b) Request from the business the **record** or **a description** of the personal information about him, her or it held by the business, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to this personal information -

I. Within a **reasonable time**;

II. At a **prescribed fee**, if any;

III. In a **reasonable manner and format**; and

IV. In a form that is **generally understandable**.

2) If the business provides the requested information as described in clause 1, the business must advise the data subject simultaneously of his, her or its right in terms of Section 24 of this Act, to **request the correction of personal information**.

3) Should the business require the data subject to **pay a fee** for the information and/or services provided in terms of clause 1(b), the business -

a) Must give the data subject a **written estimate of the fee before** providing the information and/or services; and

b) May require the data subject to **pay a deposit for all or part** of the fee prior to any requested information and/or services provided.

4) The business must ensure that it complies with the provisions of **Part 2 and Part 3 of Chapter 4 of the Promotion of Access to Information Act**, prior to disclosing information to the data subject. It is crucial that the business consult with its legal advisor to establish whether the personal information required by the data subject does not have a restriction or partial restriction prior to it being disclosed.

5) If the business receives a **written request for access to personal information**, the business must first establish which part of the information may not be disclosed, as every other part of the information must be disclosed.

8.2 Correction of personal information (Section 24)
Note to the Information Officer:
1) The business must take note that the data subject **may in writing** and with **sufficient identification**, request the business to:

a) **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**; or

b) **Destroy** or **delete** a record of personal information about the data subject that the business is no longer authorised to retain in **terms of Section 14 of this Act**.

2) If the business receives such a request from the data subject as discussed in clause 1(a) and (b), the business must as **soon as possible**:

a) **Correct** the information;

b) **Destroy** or **delete** the information;

c) Provide the data subject, to his, her or its satisfaction, with **credible evidence** in support of the information; or

d) If an agreement cannot be reached between the business 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.

3) The business should take note:
If changes have been made on request of the data subject to his, her or its personal information, that an **obligation exists on the business** to **disclose those changes** to all responsible parties, persons or bodies to whom these personal information has been disclosed, providing the changed information has an impact on decisions that have been or will be taken in respect of the data subject.
4) It is further important that the business **notify the data subject**, who has made a request in terms of clause (1), of the action taken as a result of the request.

8.3 Manner of access (Section 25)
Note to information Officer:
1) The business must ensure that any request from a data subject in terms of Section 23 of this Act, **must adhere to the stipulations of Section 18 and 53 of the Promotion of Access to Information Act**.

a) **Section 18 stipulates**:

I. "A **request for access** must be made in the prescribed form to the Information Officer of the **public body** concerned at his or her address or fax number or electronic mail address.

II. The form for a request of access prescribed in (a) must at least require the requester concerned -

- To **provide sufficient particulars** to enable an official of the public body concerned to identify the record or records requested and the requester;
- To indicate which **applicable form of access** is required;
- To state whether the record concerned is preferred in a **particular language**;
- To specify a **postal address** or fax number of the requester in the Republic;
- If, in addition to a written reply, the **requester wishes to be informed of the decision on the request** in any other manner, to state that manner and the necessary particulars to be so informed; and
- If the request is made on behalf of a person, to **submit proof of the capacity** in which the requester is making the request, to the reasonable satisfaction of the information officer.

III. An individual who, because of **illiteracy** or a **disability** is unable to make a request for access to a record of a public body in accordance with clause (a), may make that **request orally**. The Information Officer of that body must reduce that oral request to writing in the prescribed form and provide a copy thereof to the requester."

b) **Section 53 stipulates**:

I. "A **request for access** to a record of a **private body** must be made in the prescribed form to the private body concerned at its address, fax number or electronic mail address.

II. The form for a request for access prescribed in clause (a) must at least require the requester concerned –

- To **provide sufficient particulars** to enable the head of the private body concerned to identify the record(s) requested and the requester;
- To indicate which **applicable form of access** is required;
- To specify a **postal address** or fax number of the requester in the Republic;
- To identify the right the requester is seeking to exercise or protect and provide an **explanation of why the requested record** is required for the exercise or protection of that right;
- If, in addition to a written reply, the **requester wishes to be informed of the decision on the request** in any other manner, to state that manner and the necessary particulars to be so informed; and
- If the request is made on behalf of a person, to **submit proof of the capacity** in which the requester is making the request, to the reasonable satisfaction of the head."

B. Processing of Special Personal Information

The business must adhere to the following provisions when special personal information is being processed.

1) **Prohibition** on processing of personal information **(Section 26)**

2) **General authorisation** concerning special personal information **(Section 27)**

3) Authorisation concerning data subject's **religious** or **philosophical** beliefs **(Section 28)**

4) Authorisation concerning data subject's **race** or **ethnic origin(Section 29)**

5) Authorisation concerning data subject's **trade union membership(Section 30)**

6) Authorisation concerning data subject's **political persuasion(Section 31)**

7) Authorisation concerning data subject's **health** or **sex life(Section 32)**

8) Authorisation concerning data subject's **criminal behaviour** or **biometric information(Section 33)**

B1. Prohibition on processing of personal information (Section 26)

Note to Information Officer:

1) The business is prohibited to process personal information collected from a data subject concerning:

a) The **religious** or **philosophical beliefs**, **race** or **ethnic origin**, **trade union membership**, **political persuasion**, **health** or **sex life** or **biometric** information; or

b) The **criminal behaviour** of a data subject to the extent that such information relates to:

I. The **alleged commission** by a data subject of any offence; or

II. **Any proceedings in respect of any offences** allegedly committed by a data subject or the disposal of such proceedings.

c) It is important to note that the **conditions of lawful processing** as stipulated and discussed in **Part A** of this document, is also applicable to the processing of **special personal information**.

d) Unless a **general authorisation** or alternatively a **specific authorisation** relating to the different types of special information apply, the business is prohibited from processing special personal information.

B2. General authorisation concerning special personal information (Section 27)

Note to Information Officer:

1) The business must note that the **prohibition on processing** personal information as stipulated in Section 26, is **not applicable** if the –

a) Data subject has provided his, her, its **consent** pertaining to the processing of the information;

b) Processing is necessary for the **establishment**, **exercise** or **defence** 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 –

I. 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;

e) Information has **deliberately** been **made public** by the data subject;

f) Provisions of **Sections 28 to 33** are complied with; or

g) Business has provided **sufficient guarantees** to ensure that the processing of special personal information **does not adversely affect the individual privacy** of the data subject to a disproportionate extent.

2) The business must note that **Section 27** provides a **general authorisation for the processing** of **special personal information**. It is therefore important to understand that, obtaining **consent** from a data subject plays a **critical part prior to processing special personal information.** However it is not the only condition on which special personal information may be processed, as discussed in Section 27.

B3. Authorisation concerning data subject's religious or philosophical beliefs (Section 28)

Note to Information Officer:

1) The business may process special personal information concerning a data subject's religious or philosophical beliefs, as referred to in Section 26, if the processing is carried out by –

a) **Spiritual or religious organisations**, or independent sections of those organisations if –

I. The information concerns data subjects **belonging** to those organisations; or

II. It is necessary to **achieve their aims** and principles;

b) **Institutions founded on religious or philosophical principles** with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or

c) Other institutions, provided that the processing is **necessary to protect** the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

2) In the cases referred to in clause 1(a), the **prohibition for processing special personal information** relating to a data subject's religion or philosophy of life of family members, **does not apply** if:

a) The **association** concerned **maintains regular contact** with those family members in connection with its aims; and

b) The family members have **not objected in writing** to the processing.

3) **Personal information** concerning a data subject's religious and philosophical beliefs may not be supplied to third parties **without the consent of the data subject**.

B4. Authorisation concerning data subject's race or ethnic origin (Section 29)

Note to Information Officer:
1) The prohibition on processing personal information concerning a data subject's race or ethnic origin, as referred to in Section 26, **does not apply if** the processing is carried out to –

a) **Identify data subject(s)** and only when this is essential for that purpose; and

b) **Comply with laws** and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

B5. Authorisation concerning data subject's trade union membership (Section 30)

Note to Information Officer:
1) The prohibition on processing personal information concerning a data subject's trade union membership, as referred to in Section 26, **does not apply to the processing by the trade union** to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union federation.

2) Furthermore, taking the aforesaid into consideration, **no personal information** may be supplied to third parties without the consent of the data subject.

B6. Authorisation concerning data subject's political persuasion (Section 31)

Note to Information Officer:
1) The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in Section 26, **does not apply to processing** by or for an institution, founded on political principles, of the personal information of –

a) Its members or employees or other persons belonging to the institution, if such processing is necessary **to achieve the aims or principles of the institution**; or

b) **Participating in the activities** of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party.

2) It is furthermore important to note that no personal information may be supplied to third parties without the **consent of the data subject**.

B7. Authorisation concerning data subject's health or sex life (Section 32)

Note to Information Officer:
1) The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in Section 26, does not apply to the processing 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, or for the administration of the institution or professional practise concerned;

b) **Insurance companies**, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for –

I. **Assessing the risk** to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;

II. **The performance of an insurance** or medical scheme agreement; or

III. **The enforcement of any contractual rights** and obligations;

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; or

f) **Administrative bodies**, pension funds, employers or institutions working for them, if such processing is necessary for –

I. **The implementation of the provisions of laws**, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or

II. **The reintegration of or support for workers** or persons entitled to benefit in connection with sickness or work incapacity.

2) Notwithstanding the above, **the information may only be processed by responsible parties** subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the business and the data subject.

3) The business authorised to process information concerning a data subject's health or sex life in terms of this section, **is not subject to an obligation** of confidentiality by virtue of office, profession or legal provision and must treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information.

4) The prohibition on processing any of the categories of personal information as referred to in Section 26, **does not apply if it is necessary to supplement** the processing of personal information concerning a data subject's health, if the main intention is to properly treat or care for the data subject.

5) Personal information concerning inherited characteristics **may not be processed** in respect of a data subject from whom the information concerned has been obtained, **unless**–

a) **A serious medical interest prevails**; or

b) **The processing is necessary for historical**, statistical or research activity.

B8. Authorisation concerning data subject's criminal behaviour or biometric information (Section33)

Note to Information Officer:
1) The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in Section 26, **does not apply** if the 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 law**.

2) The **processing of information concerning personnel in the service** of the responsible party must take place in accordance with the rules established in **compliance with labour legislation**.

3) The prohibition on processing any of the categories of personal information referred to in Section 26, **does not apply if such processing is necessary to supplement** the processing of information on criminal behaviour or biometric information permitted by this Act.

C. Processing of Personal Information of Children

1) Prohibition on processing personal information of children **(Section 34)**

2) General authorisation concerning personal information of children **(Section 35)**

C1. Prohibition on processing personal information of children (Section 34)

Note to Information Officer:
1) It is important to note that the business may not process personal information concerning a **child.**

2) In terms of this Act a "child", means a natural person **under the age of 18 years** who is not legally competent, when determining the parameters of the processing of personal information of children.

3) The business is prohibited from processing personal information of children, unless **one of the conditions** set out in Section 35 is applicable.

C2. General authorisation concerning personal information of children (Section 35)

Note to Information Officer:
1) The prohibition on processing personal information of children, as referred to in Section 34, **does not apply** if the processing is –

a) Carried out with the prior **consent** of a competent person;

b) Necessary for the **establishment**, **exercise** or **defence** 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 –

I. the purpose serves a **public interest** and the processing is necessary for the purpose concerned; or

II. 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; or

e) Of personal information which has **deliberately** been **made public** by the child with the consent of a competent person.

2) **It is important to note that Section 35 provides a general authorisation for the processing of personal information of children. It is further important to note that consent is not the only condition on which personal information of children may be processed.**

D. Rights of Data Subjects regarding Direct Marketing by means of unsolicited electronic communication, Directories and Automated decision making

1) Direct marketing by means of unsolicited electronic communications **(Section 69)**

2) Directories **(Section 70)**

3) Automated decision making **(Section 71)**

D1. Direct Marketing by means of unsolicited electronic communication (Section 69)

Note to Information Officer:
1) 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 business**.

2) The business may approach a data subject **only once** in order to request the consent of that data subject and only if the data subject has not previously withheld such consent.

3) The data subject's consent must be requested in the prescribed manner and form.

4) The business may only process the personal information of a data subject who is a customer of the business if –

a) the business **has obtained the contact details** of the data subject in the context of the sale of a product or service;

b) the purpose of direct marketing is through the **business'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 –

I. at the time when the information was collected; and

II. on the occasion of each communication with the data subject for the purpose of direct marketing if the data subject has not initially refused such use.

5) Any communication for the purpose of direct marketing must contain –

a) **details of the identity of the sender** or the person on whose behalf the communication has been sent; and

b) **an address or other contact details** to which the recipient may send a request that such communications cease.

Important:

1.1) The business is reminded that a **data subject must consent** to the processing of his, her or its personal information for the purposes of direct marketing.

1.2) The business is allowed to approach the data subject by whatever means, **only once**, in order to obtain the consent of the data subject for the purposes of direct marketing.

1.3) The data subject must be given a reasonable opportunity to object to the processing of his, her or its personal information when the information is collected, and on any occasion that the information is used for the purpose of marketing if the data subject has not already refused to allow use of the information for this purpose.

1.4) In the event that the data subject objects, any further processing of the information for this purpose would be a breach of this Act.

D2. Directories (Section 70)

Note to Information Officer:
1) If the business has data subjects who are subscribed 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 the business must inform the data subject(s), free of charge and before the information is included in the directory –

a) of the **purpose of the directory**; and

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

2) The business must give the data subject 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.

3) If the personal information of data subjects who are subscribed to a fixed or mobile public voice telephony services and have been included in a public subscriber directory in conformity with the conditions for the lawful processing of personal information prior to the commencement of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic version, after having received the information required by clause (1).

D3. Automated decision making (Section 71)

Note to Information Officer:

1) The business may not hold the data subject liable upon making a decision **which may result in legal consequences** for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preference or conduct.

2) The abovementioned does not apply if the decision –

a) **has been taken in connection with the conclusion or execution of a contract**, and –

I. the request of the data subject in terms of the **contract has been met**; or

II. **appropriate measures have been taken** to protect the data subject's legitimate interests; or

b) **is governed by a law or code of conduct** in which appropriate measures are specified for protecting the legitimate interests of data subjects.

3) It is important to note that appropriate measures must –

a) provide an opportunity for a data subject to make representations.

b) require the business to provide a data subject with **sufficient information about the underlying logic** of the automated processing of the information relating to him, her or it to enable him, her or it to make representations.

Important:

3.1) There have been instances where the **results of decisions made by computers are influenced by incorrect data**, incomplete data or by circumstances that are not taken into account when programming the basis on which the computer may make an automated decision.

3.2) This section of the Act confers upon the data subject the **right to be provided with an opportunity to make representations** about a decision and require information pertaining to the underlying logic on which the processing of the information occurred.

E. Transborder Information Flows

1. Transfer of personal information outside the Republic of South Africa **(Section 72)**

E1. Transfer of personal information outside Republic (Section 72)

Note to Information Officer:
1) The business may **not transfer personal information** about a data subject **to a third party who is in a foreign country unless** –

a) the recipient (third party) of the personal information is subject to a **law**, binding corporate rules or binding agreement which **provide an adequate level of protection** that –

I. **effectively upholds principles for reasonable processing** of personal information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

II. **includes provisions**, **that are substantially similar to this Act**, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

b) the data subject **consents** to the transfer;

c) the transfer is **necessary for the performance of a contract** between the data subject and the business, or for the implementation of pre-contractual measures taken in response to the data subject's request;

d) the transfer is **necessary for the conclusion or performance of a contract** concluded in the **interest** of the data subject between the business and a third party; or

e) the transfer is for **the benefit of the data subject**, and –

I. it is **not reasonably practicable to obtain** the consent of the data subject to that transfer; and

II. it if was **reasonably practicable to obtain** such consent, the data subject would be likely to give it.

2) The business has an obligation to ensure that where personal information of a data subject is transferred to a third party in a foreign country, that this country has adequate levels of protection to ensure the privacy of the data subject. This will result in obtaining a service level agreement that stipulates the levels of protection applicable, prior to transferring personal information of a data subject to the third party.

F. Prior Authorisation

1) Processing subject to prior authorisation **(Section 57)**

2) The business to notify the Regulator **(Section 58)**

F1. Processing subject to prior authorisation (Section 57)

Note to Information Officer:
1) The business must obtain authorisation from the Regulator, prior to processing any personal information, if the business has the intention to –

a) process any **unique identifiers** of data subjects –

I. for **a purpose other than** the one for which the identifier was specifically intended at collection; and

II. with the **aim of linking the information** together with information processed by other businesses;

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**; or

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.

Important:

1.1) The business must obtain prior authorisation from the Regulator only **once** and not each time that personal information is received or processed, **except where the processing departs** from that which has been authorised.

F2. The business to notify the Regulator (Section 58)

Note to Information Officer:
1) The business **may not conduct any 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.

2) If the business has requested prior authorization as discussed in Section 57, **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.

3) Should the Regulator decide that a more detailed investigation is required based on the request to prior authorization from the business, the **Regulator must indicate the period within which it plans on conducting this investigation**, which period **must not exceed 13 weeks.**

4) If the more detailed investigation has been concluded, **the Regulator must issue a statement concerning the lawfulness of the information processing**.

5) Should the Regulator find, based on the request of prior authorization from the business, **that the processing of the personal information is not lawful**, **an enforcement notice** will be served in terms of Section 95 of this Act.

Important:

2.1) If the business has suspended its processing of personal information while awaiting the outcome of the Regulator's decision to proceed, and the business does not receive the Regulator's decision within the said time limits, the business may presume a decision in its favour and **continue** with its processing.

G. Supervision – Information Regulator

1. Establishment of Information Regulator **(Section 39)**

2. Powers, duties and functions of the Regulator **(Section 40)**

3. Regulator to have regard to certain matters **(Section 44)**

G1. Establishment of Information Regulator (Section 39)

1.1) The business must take note that the Information Regulator is established as a juristic person by this Act, which:

a) has **jurisdiction throughout the Republic of South Africa**;

b) **is independent** and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice;

c) **must exercise its powers** and perform its functions in accordance with this Act and the Promotion of Access to Information Act; and

d) **is accountable** to the National Assembly.

1.2) Therefore, taking the aforesaid into consideration, the Information Regulator acts **independently** of government or a political party, is accountable to the National Assembly and is required to be impartial and perform its functions and exercise its powers without fear, favour or prejudice.

G2. Powers, Duties and Functions of the Regulator (Section 40)

Important:

2.1) It is important for you as an Information Officer to understand the powers, duties and functions of the Information Regulator, which include the following:

a) To **provide education**, including the promotion of understanding and acceptance of the conditions of lawful processing of personal information;

b) To **monitor and enforce compliance** through the powers vested in it by the legislation;

c) To **consult with interested parties** on a national and international basis;

d) To **handle and investigate complaints**;

e) To **conduct research** and report to Parliament on international developments;

f) To **assist in the establishment and development of codes of conduct**;

g) To **facilitate cross-border cooperation** in the enforcement of privacy laws with other jurisdictions; and

h) To **generally do everything necessary to fulfil these duties**, and foster a culture which protects personal information in South Africa."

Note to Information Officer:
1) Complaints may be lodged with the Information Regulator, whereafter the Information Regulator will investigate the alleged offence or contravention in accordance with the stipulations of this Act.

G3. Regulator to have regard to certain matters (Section 44)

Important:

3.1) During the fulfilment of the Information Regulator's duties and functions, it must take the following into consideration:

a) Have due regard for the **conditions for the lawful processing** of personal information;

b) Have due regard for **the protection of all human rights** and **social interests** that compete with privacy, including the general desirability of a free flow of information recognition of the legitimate interests of the public and private bodies in achieving their objectives in an efficient way;

c) Take account of **international obligations** accepted by South Africa; and

d) Consider any developing general **international guidelines** relevant to the better protection of individual privacy.

Note to Information Officer:
1) The Regulator will not only assess whether the lawful conditions of processing personal information have been complied with before determining an outcome of a complaint that has been lodged, but will also take (b) – (d) mentioned above into consideration in order to ensure that this Act is being enforced fairly and reasonably.

H. Enforcement and Penalties

1) Complaints to the Regulator

2) Penalties

H1. Complaints to the Regulator

Important:

1) The business must take note that:

a) Any contravention and/or dispute in terms of this Act may be lodged to the Information Regulator, which possesses the authority to **lodge an investigation and subsequently issue information-, enforcement- and infringement notices**.

b) If the business receives an **information- or enforcement notice**, the business may **lodge an appeal to the High Court** having jurisdiction for the setting aside or variation of the notice, **within 30 days after receiving the notice**.

Risk:

It is important to note that the data subject is not limited to lodge a complaint only to the Information Regulator, but may decide to institute a **civil action** for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act, whether or not there is intent or negligence on the part of the business. The data subject may request the Information Regulator to institute civil proceedings on his, her or its behalf.

Risk:

A court issuing any order for damages must order it to be published in the Government Gazette and by such other appropriate public media announcement as the court considers appropriate.

H2. Penalties

Note to Information Officer:
1) It is important to note, that should the business or its responsible party be convicted of an offence in terms of this Act, the business or its representative will be liable –

a) to **a fine or to imprisonment for a period not exceeding 10 years**, or to both a fine and such imprisonment in the following circumstances:

I. **Obstruction** of Regulator – Section 100;

II. **Failure to comply** with enforcement notice – Section 103(1);

III. **False evidence** given by witnesses under oath – Section 104(2);

IV. **Unlawful acts by the business** in connection with account numbers – Section 105(1);

V. **Unlawful acts by third parties** in connection with account numbers – Section 106;

b) to **a fine or to imprisonment for a period not exceeding 12 months**, or to both a fine and such imprisonment in the following circumstances:

I. **Failure to notify** processing subject to prior authorisation – Section 59;

II. **Breach of confidentiality** – Section 101;

III. **Obstruction of execution** of warrant – Section 102;

IV. **Failure to comply** with information notice – Section 103(2);

V. **Witness failing to comply** with the terms and conditions of a summons.

Important:

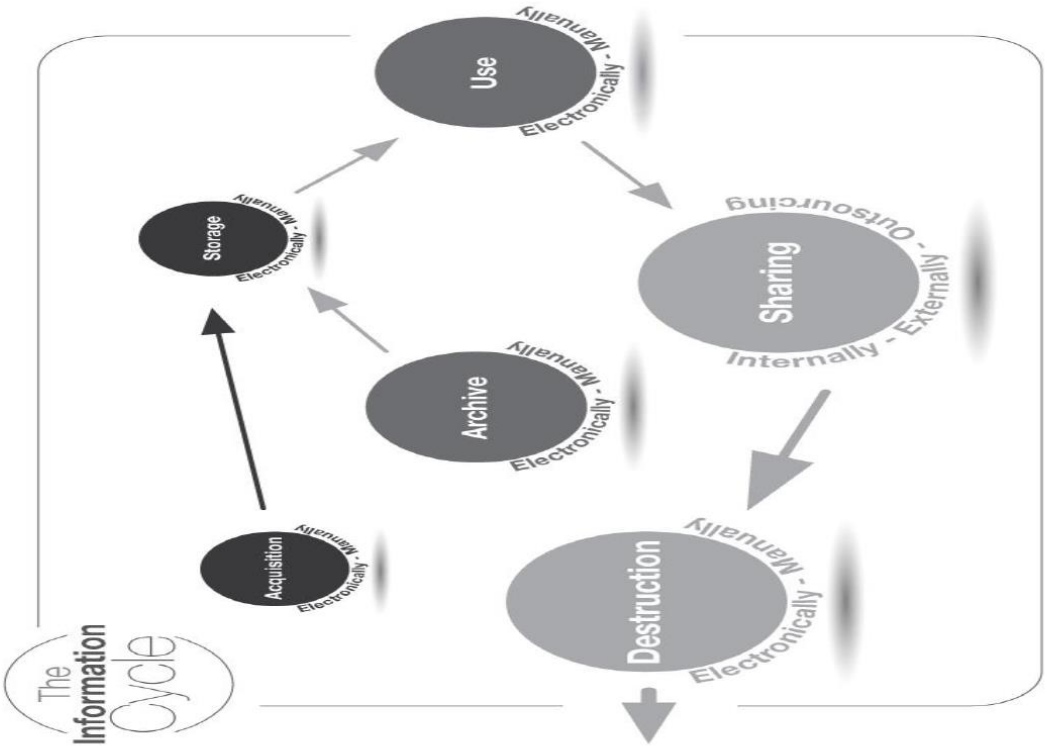
2.1) The amount of an administrative fine that may be imposed on the business by the Information Regulator may not exceed **R 10 million.**

I. Summary

1) Information Cycle

2) What is the next step?

3) Areas of concern



I2. What is the next step?

1) **Take Stock** - Know what personal information you have in your files and on your computers.

2) **Scale Down** – Keep only what you need for your business – **PURPOSE SPECIFIC**! This will mean that terms and conditions will have to be redrafted.

3) **Lock It** – Protect the information you keep. Physical security, electronic security, training of employees and the security practises of contractors/service providers. This will include new policies drafted and implemented, e.g. Access Control Policy, Data Retention Policy, Data Destruction Policy, Handheld & Mobile Device Policy, Access Control Policy.

4) **Pitch It** – Properly dispose (de-identify) of personal information that you no longer need, where the **PURPOSE** for collecting no longer exists.

5) **Plan Ahead** – Create an action plan to respond to security incidents and have quarterly meetings with the Deputy Information Officer(s) to discuss, establish and ensure that no information breaches have occurred and the current security safeguards remains adequate to address possible risk areas.

Important:

2.1) It is suggested that the Information Officer conduct regular meetings with his/her Deputy Information Officer(s) to ensure the above steps are adhered to. These regular meetings should include discussions pertaining to:

a) Additional risk areas;

b) Policy amendments;

c) Pitfalls;

d) Information breaches;

e) Policy implementations;

f) Training of relevant staff;

g) Roles and responsibilities of Information Officer and Deputy Information Officer(s) and;

h) Implementation of the proposed guidelines as stipulated in the Information Guide.

Areas of concern pertaining to Lawnpro Head Office (Pty) Ltd.

Lawpro Head Office Pty Ltd collects personal information from clients and even more so from employees. It's important that you protect such in accordance with the POPI Act to avoid any penalties or fines.

Subsequent to the first consultation held, we have compiled a list of areas of concern regarding the current status in which the Company processes (uses) personal information.

It is highly recommended to address same as a matter of urgency in order to comply with the provisions of the Act regulating processing of personal information, thus avoiding compliance orders, fines, compensation claims and in some cases imprisonment.

Please note that the business is a **Responsible Party,** which is a body which **collects determines the purpose/means of processing of personal information (**i.e.: decides what happen with the personal information**)**. For example, a Responsible Party receives personal information directly from data subjects such as employees, suppliers or clients. We have however highlighted a few areas (below) which you may wish to review in order to ensure compliance.

Requesting Personal Information

We have been advised that **Lawnpro Head Office Pty Ltd** may not always disclose the **purpose** for the collection of personal information. Please note that this does not comply with the requirements of Section 13 of POPI, which indicates that the Responsible Party must ensure that the data subject, in accordance with Section 18(1), is made aware of the purpose of the collection of the information unless the provisions of Section 18(4) is not applicable. Please therefore ensure that the purpose of the collection complies with the requirements of Section 13 and Section 18 of POPI.

Section 12- "Collection directly from data subject"

All information collected and processed must be collected directly from the data subject. Unless otherwise allowed in section 12 (exclusions). Please take note that the Protection of Personal Information Act (POPIA) requires that processing of personal information be lawful and comply with the 8 lawful conditions as envisaged in chapter 3 of the Act. Please be informed that the processing of the personal information you do, will be discussed extensively when we conduct the Protection of Personal Information Implementation. Note that in the meantime, the following clause may be inserted at the bottom of the form.

Filing and Storage of Personal Information:

Section 19 – "Security measures on integrity and confidentiality of personal information"

It is important that all records of personal information be properly safeguarded by adequate security measures. We advise that the security measures pertaining to all hard copy and electronic files containing personal information be revisited to ensure compliance with this section.

Hard Copy Documentation:

We have been advised that the company stores personal information in both:

a) In order to be POPI compliant herein you will have to ensure that the access to those documents are only limited to those employees that require access to those documents per the work duties.

Electronic:
We have been advised that personal information is stored on company computers which are password protected. In order to meet the pre-requisite guidelines requiring businesses to safeguard information entrusted to it, the Responsible Party must ensure that:

- Employees do not share passwords;
- Passwords are updated regularly;
- Computers have software installed allowing review capabilities;
- Anti-virus programs have been installed;
- Software is encrypted;
- There are sufficient firewalls in place.

Data Retention:

Section 14 - "Retention and restriction of records"

All records of personal information should be de-identified (not to be recalled) as soon as the purpose for its collection has been achieved unless otherwise allowed in section 14.

We have been advised that it retains documents **indefinitely**. Please note that documentation bearing personal information should only be stored for the period necessary for achieving/fulfilling the purpose of its collection. The aforementioned requirement relates to information stored both via hard copy and electronically. Once a document no longer has a purpose that is when it should be destroyed.

Note: We understand that certain products have manufacturer's warranties which would then become the purpose for holding onto certain personal information.

Data destruction:
We were advised that **Lawnpro Head Office Fitness Pty Ltd** has no set method of disposal of documentation. To be complaint you will need to delete personal information stored electronically from the servers and computers/laptop and the hard copies should be shredded.

Employment contracts:

Should the employment contract utilised by **Lawnpro Head Office Pty Ltd** not make provision for the use of an employee's personal information, you may need to include the following in the contract or as an addendum:

Consent to use of Personal Information

1. The Employee hereby consents to the collection, processing and further processing of the Employee's personal information by the Company, for the purpose of securing and further facilitating the Employee's employment with the Company.
2. Without derogating from the generality of the aforementioned, the Employee consents to the Company's collection and processing of personal information pursuant this clause insofar as personal information of the Employee is contained in relevant electronic communications and/or manual collection.
3. The Employee is hereby notified of the purpose and reason for the collection and processing of such personal information.
4. The Employee undertakes to make available to the Company all necessary personal information required by the Company for the purpose of securing and further facilitating the Employee's employment with the Company.

Signed at _____ on this _____ day of _____ 2024.

As witnesses:

1. _____ **_____**
Employee

2. _____ **_____**
Employer

The POPI Act also applies to all personal information of staff members. The information below are guidelines as to how to process personal information of prospective employees, current employees and persons who have left your employ:

Recruitment Records:

- When advertising a vacancy, only request personal information which is relevant to the recruitment decision.
- Determine whether all questions are relevant to all applicants.
- Remove questions which are only relevant to successful applicants (e.g. banking details).
- Ensure that no recruitment record is retained beyond the statutory period in which a claim arising from the recruitment process may be brought unless there is a clear business reason for exceeding this period.
- Consider sorting any recruitment information that is to be held longer than the period necessary for responding to claims.
- Ensure that applicants are advised that application forms and/or supplementary documentation will be retained unless they specifically request the return or destruction thereof.

Keeping General Records:

- Request employees to check their records for accuracy and ensure that necessary amendments are made to update records.
- Make provision to amend any details which are incorrect on individual employees' files.
- Incorporate accuracy, consistency and validity checks into systems.
- Remember that legal responsibility for data protection compliance rests with users rather than suppliers of systems.

Disciplinary Procedures:

Employers must:

- assess the company's disciplinary and grievance procedures and decide whether the existing procedures comply with the Act.
- ensure that whomever (whether an employee of the company or an outsourced company) is responsible for collecting information to be used is aware that the proposed legislation grants employees the right to access any personal information and their duty to disclose the purpose for which they are gathering the information.
- note that they should not use or access information collected for the purposes of disciplinary or dismissal proceedings if such access or use would be incompatible with the purpose(s) that the information was obtained for.

Destruction, use, modification or disclosure of data:

- Ensure that security standards make provision for potential risks to information, such as unauthorized access to, accidental loss of, destruction of, or damage to employment records.
- Institute a system by utilizing secure cabinets, access controls and passwords to ensure that employees can only gain access to employment records if they have a legitimate business need to do so. Check whether computerized systems that retain personal information currently have audit trail capabilities. If they do, check that the audit trail is enabled.
- Take account of the risks of transmitting confidential employee information by fax or email.

References Requests:

- Do not provide confidential references about an employee unless you are sure that this is the employee's wish.
- Set out a clear company policy stating who can give corporate references, in what circumstances, and the policy that applies to the granting of access to them.
- Make anyone who is likely to become a referral aware of this policy.
- As part of the policy, include a requirement that all those giving corporate references must be satisfied that the employee wishes the reference to be provided.
- As part of an Exit Policy, include on file a record of whether the employee wishes references to be provided after he/she has left.

Operators:

Lawnpro Head Office Ltd t/a uses the services of Operators which are allowed access personal information received by the Responsible party. Please ensure that a written agreement is concluded between the parties regulating the use and storage of personal information while such information is under the service providers' control. If there is no written agreement in place consider using the 'Data Processing Agreement' to protect the School in this type of situations.

Ie: this would need to be in place with:

- BB3 Marketing

“Annexure A”

DATA PROCESSING AGREEMENT

ENTERED INTO BETWEEN:
_____, having its principal place of business in Pretoria at

_____.
(hereinafter to be referred to as: the “Responsible Party”),
AND
_____, having its principal place of business in

_____ at _____
(hereinafter to be referred to as: the “Operator”).

HEREBY AGREE AS FOLLOWS:

1. Definitions:

“Data subject”: means the person to whom personal information relates.
“Information officer”: of, or in relation to, a –
a) Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of this Act; or
b) Private body means the head of a private body as contemplated in Section 1, of The Promotion of Access to Information Act.
“Operator”: means a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party.
“Personal information”: means 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, 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 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.

"Processing": means 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.

"Promotion of Access to Information Act": means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
"Protection of Personal Information Act": means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
"Pseudonymisation": It requires that personal data must not be able to be attributed to a specific data subject without the use of additional information kept separately, and subject to "technical and organisational measures.
"Responsible Party": means 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.

2. Subject matter of this Data Processing Agreement

2.1. This Data Processing Agreement applies to the processing of personal information subject to the Protection of Personal Information Act (hereinafter referred to as POPIA) in the scope of the ***[insert type of agreement***] entered into on [**date]** between the parties.

2.2. Insofar as the Operator will be processing personal information subject to POPIA on behalf of the Responsible Party in the course of the performance of the ***[insert type of agreement]*** with the Responsible Party, the terms of this Data Processing Agreement shall apply. In the event of a conflict between any provisions of the ***[Insert type of agreement]*** and the provisions of this Data Processing Agreement, the provisions of this Data Processing Agreement shall govern and control. An overview of the categories of personal information, the categories of Data Subjects, and the nature and purposes for which the personal information are being processed is provided in Annexure 2.

3. The Responsible Party and the Operator

3.1. Subject to the provisions of the ***[insert type of agreement]***, to the extent that the Operator's personal information processing activities are not adequately described in the [***insert type of agreement***], the Responsible Party will determine the scope, purposes, and manner by which the personal information may be accessed or processed by the Operator. The Operator will process the personal information only as set forth in the Responsible Party's written instructions and no personal information will be processed unless explicitly instructed by the Responsible Party.

3.2. The Operator will only process the personal information on documented instructions of the Responsible Party to the extent that this is required for the provision of the services. Should the Operator reasonably believe that a specific processing activity, beyond the scope of the Responsible Party's instructions, is required to comply with a legal obligation to which the Operator is subject, the Operator shall inform the Responsible Party of that legal obligation and seek explicit authorization from the Responsible Party before undertaking such processing. The Operator shall never process personal information in a manner inconsistent with the Responsible Party's documented instructions.

3.3. The parties have entered into a ***[insert type of agreement]*** in order to benefit from the capabilities of the Operator in securing and processing the personal information for the purposes set out in Annexure 2. The Operator shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, provided that all such discretion is compatible with the requirements of this Data Processing Agreement, in particular the Responsible Party's written instructions.

3.4. The Responsible Party warrants that it has all necessary rights to provide the personal information to the Operator for the processing to be performed in relation to the services, and that one or more justification grounds set forth in POPIA support the lawfulness of the processing. To the extent required by the POPIA, the Responsible Party is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another justification ground is set forth in POPIA supports the lawfulness of the processing, that any necessary Data Subject consent to the processing is obtained, and for ensuring that a record of such consent is maintained. Should such a consent be revoked by a Data Subject, the Responsible Party is responsible for communicating the fact of such revocation to the Operator, and the Operator remains responsible for implementing the Responsible Party's instruction with respect to the processing of that personal information.

4. Confidentiality

4.1. Without prejudice to any existing contractual arrangements between the parties, the Operator shall treat all personal information as confidential and it shall inform all its employees, agents and/ or approved sub-Operators engaged in processing the personal information of the confidential nature of the personal information. The Operator shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

5. Security

5.1. Taking into account the industry norm, the costs of implementation, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the Responsible Party and Operator shall implement appropriate, reasonable technical and organisational measures to ensure a level of security of the processing of personal information appropriate to the risk. These measures shall include, at a minimum, the security measures agreed upon by the parties in Annexure 3.

5.2. Both the Responsible Party and the Operator shall maintain written security policies that are fully implemented and applicable to the processing of personal information. At a minimum, such policies should include assignment of:

- Internal responsibility for information security management;
- Devoting adequate personnel resources to information security;
- Carrying out verification checks on permanent staff who will have access to the personal information;
- Requiring employees, vendors and others with access to personal information to enter into written confidentiality agreements, and
- Conduct training to make employees and others with access to the personal information aware of information security risks presented by the Processing.

5.3. The Operator's adherence to either an approved code of conduct or to an approved recognised security certification standard, may be used as an element by which the Operator may demonstrate compliance with the requirements set out, provided that the requirements contained in Annexure 3 are also addressed by such code of conduct or recognised security certification standard.

6. Improvements to Security

6.1. The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Operator will therefore evaluate the measures as implemented on an on-going basis in order to maintain compliance with the requirements set out in POPIA.

6.2. Where an amendment to the ***[insert type of agreement]*** is necessary in order to execute a Responsible Party's instruction to the Operator to improve security measures as may be required by changes in terms of the POPIA from time to time, the parties shall negotiate an amendment to the ***[insert type of agreement]*** in good faith.

7. Information Transfers

7.1. The Operator shall promptly notify the Responsible Party of any planned permanent or temporary transfers of personal information to a third country, without an adequate level of protection, and shall only perform such a transfer after obtaining authorisation from the Responsible Party, which may be refused at its own discretion. Annexure 4 provides a list of transfers for which the Responsible Party grants its authorisation upon the conclusion of this Data Processing Agreement.

8. Information Obligations and Incident Management

8.1. When the Operator becomes aware of an incident that has a material impact on the processing of the personal information that is the subject of the ***[insert type of agreement here]***, it shall promptly notify the Responsible Party about the incident, shall at all times cooperate with the Responsible Party, and shall follow the Responsible Party's instructions with regard to such incidents, in order to enable the Responsible Party to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

8.2. The term “incident” used in paragraph 8.1 shall be understood to mean in any case:

(a) a complaint or a request with respect to the exercise of a Data Subject’s rights in terms of POPIA;

(b) any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the personal information;

(c) any breach of the security and/or confidentiality as set out in this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the personal information, or any indication of such breach having taken place or being about to take place;

(d) where, in the opinion of the Operator, implementing an instruction received from the Responsible Party would violate applicable laws to which the Responsible Party or the Operator are subject.

8.3. The Operator shall at all times have in place written procedures which enable it to promptly respond to the Responsible Party about an incident. Where the incident is reasonably likely to require a data breach notification by the Responsible Party in terms of the POPIA, the Operator shall implement its written procedures in such a way that it is in a position to notify the Responsible Party without undue delay after the Operator becomes aware of such an incident.

8.4. Any notifications made to the Responsible Party shall be addressed to the employee of the Responsible Party whose contact details are provided in Annexure 1 of this Data Processing Agreement and, in order to assist the Responsible Party in fulfilling its obligations in terms of the POPIA, should contain:

(a) a description of the nature of the incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal information records concerned;

(b) the name and contact details of the Operator’s Information Officer or another contact point where more information can be obtained;

(c) a description of the possible consequences of the incident;

(d) a description of the measures taken or proposed to be taken by the Operator to address the incident including, where appropriate, measures to mitigate its possible adverse effects; and

(e) if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

9. Contracting with Sub-Operators

9.1. The Operator shall not subcontract any of its service-related activities consisting (partly) of the processing of the personal information or requiring personal information to be processed by any third party without the prior written authorisation of the Responsible Party.

9.2. The Responsible Party authorises the Operator to engage the sub-Operators listed in Annexure 4 for the service-related personal information processing activities described in Annexure 2. Operators shall inform the Responsible Party of any addition or replacement of such sub-Operators giving the Responsible Party an opportunity to object to such changes. If the Responsible Party timely sends the Operator a written objection notice, setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve the Responsible Party's objection. In the absence of a resolution, the Operators will make commercially reasonable efforts to provide Responsible Party with the same level of service described in the ***[insert type of agreement here]***, without using the sub-Operator to process personal information. If the Operator's efforts are not successful within a reasonable time, each party may terminate the portion of the service which cannot be provided without the sub-Operator, and the Operator will be entitled to a pro-rated refund of the applicable service fees.

9.3. Notwithstanding any authorisation by the Responsible Party within the meaning of the preceding paragraph, the Operator shall remain fully liable vis-à-vis the Responsible Party for the performance of any such sub-Operator that fails to fulfil its information protection obligations.

9.4. The Operator shall ensure that the sub-Operator is bound by data protection obligations compatible with those of the information processed in terms of this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its sub-Operators the obligation to implement appropriate, reasonable technical and organizational measures in such a manner that the processing will meet the requirements of the POPIA.

10. Returning or Destruction of Personal Information

10.1. Upon termination of this Data Processing Agreement, upon the Responsible Party's written request, or upon fulfilment of all purposes agreed in the context of the services whereby no further processing is required, the Operator shall, at the discretion of the Responsible Party, either delete, destroy or return all personal information to the Responsible Party and destroy or return any existing copies.

10.2. The Operator shall notify all third parties supporting its own processing of the personal information of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the personal information or return the personal information to the Responsible Party, at the discretion of the Responsible Party.

11. Assistance to the Responsible Party

11.1. The Operator shall assist the Responsible Party by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Responsible Party's obligation to respond to requests for exercising the data subject's rights in terms of the POPIA.

11.2. Taking into account the nature of processing and the information available to the Operator, the Operator shall assist the Responsible Party in ensuring compliance with obligations pursuant to Section 4 (Security), as well as other Responsible Party obligations in terms of POPIA that are relevant to the information processing described in Annexure 2, including notifications to the Information Regulator or to Data Subjects.

11.3. The Operator shall make available to the Responsible Party all information necessary to demonstrate compliance with the Responsible Party's obligations and allow for and contribute to audits, including inspections, conducted by the Responsible Party.

12. Duration and Termination

12.1. This Data Processing Agreement shall come into effect on the effective date of the ***[insert agreement type here]***.

12.2. Termination or expiration of this Data Processing Agreement shall not discharge the Operator from its confidentiality obligations in terms of this agreement.

12.3. The Operator shall process personal information until the date of expiration or termination of the ***[Insert type of agreement here]***, unless instructed otherwise by the Responsible Party, or until such data is returned or destroyed on instruction of the Responsible Party.

13. Miscellaneous

13.1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the **[insert type of agreement here]**, the provisions of this Data Processing Agreement shall prevail.

13.2. This Data Processing Agreement is governed by the laws of ***[Country]***. Any disputes arising from or in connection with this Data Processing Agreement shall be brought exclusively before the competent court of ***[Jurisdiction]***.

Signed for and on behalf of the Responsible Party:
Name:
Title:
Date:

Signed for and on behalf of the Operator:
Name:
Title:
Date:

Annexure 1:
Contact information of the information officer of the Responsible Party

Name and Surname:
Contact number:
Email address:

[Contact information]
Contact information of the information officer of the Operator.

Name and Surname:
Contact number:
Email address:

Annexure 2:
Types of personal information that will be processed in the scope of the ***[insert agreement type here]***:

Categories of Data Subjects:

Nature and purpose of the information processing:

Annexure 3: Security Measures

Operator shall:
1. Ensure that the personal information can be accessed only by authorized personnel for the purposes set forth in Annexure 2 of this Data Processing Agreement;

2. Take all reasonable measures to prevent unauthorized access to the personal information through the use of appropriate physical and logical (passwords) entry controls, securing areas for information processing, and implementing procedures for monitoring the use of information processing facilities;

3. Build in system and audit trails;

4. Use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;

5. Account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of personal information;

6. Ensure pseudonymisation and/or encryption of personal information, where appropriate;

7. Maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

8. Maintain the ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident;

9. Implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal information;

10. Monitor compliance on an ongoing basis;

11. Implement measures to identify vulnerabilities with regard to the processing of personal information in systems used to provide services to the Responsible Party;

12. Provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

Annexure 4:

Transfers to sub-Operators in third countries, including outside the Republic of South Africa, without an adequate level of protection for which the Responsible Party has granted its authorisation:
Sub-Operator:

Lawnpro Head Office:

Registration number:
Contact number:
Email Address:
Country: