INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Address: Braampark Forum III, 33 Hoofd St,
Braampark, Johannesburg, 2017
Fax: 0865003351
E-mail: VarSewlal@justice.gov.za

23 June 2021

NOTICE IN TERMS OF SECTION 61(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA): NATIONAL RADIOLOGY SERVICES INC

In terms of the provisions of section 61 (2) of POPIA, the Information Regulator gives notice that the Regulator is in receipt of a code of conduct from National Radiology Services Inc, a medical service provider in the Radiology industry. The code deals with how personal information will be processed by the company. Affected persons are invited to submit written comments to the Regulator (email address: codes.IR@justice.gov.za) till the 13th August 2021. A notice will also be published in the Government Gazette in compliance with section 61 (2) of POPIA.

National Radiology Services Inc.
• Reg. No: 2004/009411/21
DIAGNOSTIC RADIOLOGISTS | DIAGNOSTIESE RADIOLOË | UDOKOTELA WE-XRAY
DR. V.K.S. BHAGWANDAS MB BCh (Wits), FCRad (SA), EDiNR (Neuroradiology) FRANZCR
DR. D.H. JOGI MB BCh (Wits), FCRad (SA), FRCR (London), MMed (Rad D) (Wits), EDiNR (Neuroradiology), EDiPNR (Peadiatric Neuroradiology)
DR. ASHESH I. RANCHOD MB BCh (Wits), FCRad (SA), EDiPNR (Peadiatric Neuroradiology) • **DR. R. NAIK** MB BCh (Wits), FCRad (SA)
DR. K. GOVENDER MB ChB (Natal), FCRad (SA) • **DR. M.N. PATEL** MB ChB (UCT), FCRad (Diag)(SA), MMed (Diag Rad) (UCT) • **DR. AMARESH I. RANCHOD** MB BCh (Wits), FCRad (SA)
DR. I. NAGDEE BSc MB BCh FCRad (SA) • **DR. K.P. KOBO** BSc. Ed (WSU), MB ChB (Mendunsa), FCRad (SA) • **DR. M. MATTHEE** MB BCh (Wits), FCRad (SA)
DR. Y. ISMAIL MB BCh (Wits). FCRad (SA) • **DR. S. PALLIAM** MB ChB (Medunsa) FC Rad (SA)
Lenmed: Tel: 011 852 8820
N17: Tel: 011 815 2814
Waterfall: Tel: 011 304 6669
Promoting Imaging Excellence
www.nationalradiologyservices.co.za
VAT No. 4840211868 • PR. NO. 038 000 014 5459 • BEE Rating Level 8
Carnival Medicross: Tel: 011 915 0540
Accounts: Tel: 010 612 0271

CODE OF CONDUCT
(POPIA)

CODE OF CONDUCT GOVERNING THE CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION BY ALISTAIR GROUP (PTY) LTD.

ISSUED IN TERMS OF SECTION 60 OF THE PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013 ("POPIA") BY THE INFORMATION REGULATOR.

Netcare B17 Private Hospital
7 Tonkmeter Road
Pollak Park, Springs
Tel: 011 815 2814 / 6409 / 2258
Fax: 011 815 1099

Waterfall City Private Hospital
Cnr Magwa Crescent & Mac Mac Avenue
Midrand
Tel: 011 304 6670 / 011 304 6669
Fax: 011 304 6806

Lenmed Health
Ahmed Kathrade Private Hospital
Off K53 Highway
Marlin Ave, Lenasia
Tel: 011 852 8820 / 1 / 2
Fax: 011 852 8823

Accounts Dept. - NRS House
12 Stirrup Lane,
Woodmead Office Park
Woodmead, 2191
Tel: 010 612 0271
Fax: 011 656 0712
ranchodnjogi@mweb.co.za

TABLE OF CONTENTS

PART A – INTRODUCTION

1. BACKGROUND OF THE COMPANY

National Radiology Services Inc. is a medical service provider in the Radiology industry with 4 practices in Gauteng.

2. COMPANY CODE OF CONDUCT (POPIA)

2.1 "Enforcement" in Chapter 10 and "Offences, Penalties and Administrative Fines" in Chapter 11 of PoPIA.

2.2 The Company will, in the drafting of and applying to the Regulator for the issue of this Code of Conduct, consult with the Information Regulator, with a view to promoting compliance with PoPIA and a consistency in the approach in this regard.

3. MANDATE AND APPLICATION

3.1 By applying to the Information Regulator for the issue of this Code of Conduct the COMPANY confirms that it is acting in terms of the mandate of all of its members at the time that the application is made.

3.2 The Company Executive Manager is mandated to, prior to the issue of this Code of Conduct, request the Information Regulator to provide rulings of interpretation on PoPIA that may affect the provisions of this Code of Conduct and to affect non-material amendments to the wording of this Code of Conduct as may be required by the Information Regulator, without further reference to the Company.

2.3 This Code of Conduct applies to the Company, in its processing of all information (by definition in PoPIA personal information) in the course of fulfilling its obligations.

4. PURPOSE

4.1 THE PURPOSE OF THIS CODE OF CONDUCT IS TO:

4.1.1 Promote appropriate practices by the Company governing the processing of personal information;

4.1.2 Encourage the establishment of appropriate agreements between members of the Company and third parties, regulating the processing of personal information as required in PoPIA and dictated by good business practice.

4.2 A further purpose of this Code of Conduct is to establish procedures for the COMPANY to be guided in their interpretation of principally PoPIA, but also other law or practices governing the processing of personal information, allowing for complaints against the Company to be considered and remedial action, where appropriate, to be taken.

5. SCOPE

5.1 THIS CODE OF CONDUCT GOVERNS:

5.1.1 The processing of personal information by the Company in compliance with PoPIA;

5.1.2 Where appropriate, agreements that may need to be concluded between the Company and third parties promoting, and to the extent possible ensuring, that personal information is processed in compliance with PoPIA;

5.1.3 The enforcement by the Company of the provisions of this Code of Conduct.

6. DEFINITIONS AND ABBREVIATIONS

6.1 RELEVANT PoPIA DEFINITIONS:

6.1.1	**‘‘Child’’**	Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decisions;
6.1.2	**‘‘Code of Conduct’’**	Means a code of conduct issued in terms of Chapter 7 of PoPIA;
6.1.3	**‘‘Competent Person’’**	Means any person who is legally competent to consent to any action;
6.1.4	**‘‘Consent’’**	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
6.1.5	**‘‘Constitution’’**	Means the Constitution of the Republic of South Africa, 1996;
6.1.6	**‘‘Data Subject**’’	Means the person to whom personal information relates;

6.1.7 ‘‘**De-identify”** In relation to personal information of a data subject, means to delete any information that;

a. Identifies the data subject;

b. Can be used or manipulated by a reasonably foreseeable method to identify the data subject;

c. Can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ‘‘de-identified’’ has a corresponding meaning;

d. “Direct marketing’’ means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

i. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

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

6.1.8 **“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;

6.1.9 **“Enforcement notice’’** means a notice issued in terms of section 95;

6.1.10 **‘‘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;

6.1.11 **‘‘Information Officer**’’ of, or in relation to, a:

a. Public body means an information officer or deputy information officer as

b. Contemplated in terms of section 1 or 17; or

c. Private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

6.1.12 **‘‘Minister**’’ means the Cabinet member responsible for the administration of justice;

6.1.13 **‘‘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;

6.1.14 **‘‘person’’** means a natural person or a juristic person;

6.1.15 **‘‘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, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person;

b. Information relating to the education or the medical, financial, criminal or employment history of the person;

c. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.

6.1.16 **‘‘Prescribed’’** means prescribed by regulation or by a code of conduct;

6.1.17 **‘‘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.

6.1.18 **‘‘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.

6.1.19 **''Promotion of Access to Information Act''** means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

6.1.20 **''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;

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.

6.1.21 **''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;

6.1.22 **''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 tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
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 any other device in which one or more visual;
vi. Images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

b. In the possession or under the control of a responsible party;

c. Whether or not it was created by a responsible party; and

d. Regardless of when it came into existence.

6.1.23 **''Regulator''** means the Information Regulator established in terms of section 39 of PoPIA;

6.1.24 **''Republic''** means the Republic of South Africa;

6.1.25 **''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;

6.1.26 **''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;

6.1.27 **''Special Personal Information''** means personal information as referred to in section 26;

6.1.28 **''This Act''** includes any regulation or code of conduct made under the Protection of Personal Information Act, 4 of 2013; and

6.1.29 **''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.

6.2 RELEVANT COMPANY DEFINITIONS:

6.2.1 **"Agreement"** includes an arrangement or understanding between or among two or more parties, which purports to establish a relationship in law between those parties;

6.2.2 **"Complainant"** means a person who has filed a complaint in terms of section 136(1);

6.2.3 **"Confidential Information"** means personal information that belongs to a person and is not generally available to or known by others;

6.2.4 **"Client/Customer/Resident/Employee"**, in respect of an agreement to which this Act applies, means:

a. The party to whom goods or services are sold to;

b. The party who is employed by the Company;

c. A person's education, employment, career, professional or business history, including the circumstances of termination of any employment, career, professional or business relationship, and related matters; or

d. A person's identity, including the person's name, date of birth, identity number, marital status and family relationships, past and current addresses and other contact details, and related matters;

6.2.5 **"Credit"**, when used as a noun, means;

a. A deferral of payment of money owed to a person, or a promise to defer such a payment; or

b. A promise to advance or pay money to or at the direction of another person.

6.2.6 **"Juristic Person"** includes a partnership, association or other body of persons, corporate or unincorporated, or a trust if:

a. There are three or more individual trustees; or

b. The trustee is itself a juristic person, but does not include a stokvel.

6.2.7 **"Magistrates' Courts Act"** means the Magistrates' Courts Act, 32 of 1944;

6.2.8 **"Organ of State"** means an organ of state as defined in section 239 of the Constitution;

6.2.9 **"Prescribed"** means prescribed by regulation;

6.2.10 **"SMS"** means a short message service provided through a telecommunication system;

6.3 CODE OF CONDUCT DEFINITIONS:

6.3.1 **"Business Days"** means all weekdays which are not proclaimed public holidays in the Republic of South Africa;

6.3.2 **"Company Executive Manager"** means the person appointed by the Company to oversee the conduct of its business.

6.4 ABBREVIATIONS:

6.4.1 **"Company"** means……;

6.4.2 **"ISMS"** means an Information Security Management System;

6.4.3 **"PAIA"** means the Promotion of Access to Information Act, 2 of 2000;

6.4.4 **"PoPIA"** means the Protection of Personal Information Act, 4 of 2013;

7. PART B OF THIS CODE OF CONDUCT DEALS WITH EACH OF:

7.1 The lawful conditions for Processing of personal information;

7.2 The Processing of special personal information; and

7.3 The Processing of personal information of children.

8. THE DUTIES AND RESPONSIBILITIES OF THE INFORMATION OFFICER:

8.1 Direct marketing by means of unsolicited electronic communications; and

8.2 Transfers of personal information outside Republic;

8.3 In Parts B and C of this Code of Conduct the relevant provisions of PoPIA are quoted in full, and are identified by being illuminated;

8.4 Immediately subsequent to the provisions referred to in 7, reference is made to Other Applicable Legislation relevant to the processing of personal information by the Company.;

8.5 Immediately subsequent to the provisions referred to in 7, Other Applicable Legislation, a brief commentary providing guidance to the Company relating to the processing of personal information in compliance with PoPIA in terms of accepted industry practices is provided.

8.6 Immediately subsequent to the commentary, the obligations of the Company to comply with PoPIA or actions or omissions that are a functional equivalent in the processing of personal information are stipulated in bold. These provisions do not substitute the stipulations of PoPIA or in any way detract from their operation and must be construed as supplementary to the provisions of PoPIA.

9. COMMENCEMENT OF THE CODE

9.1 This Code of Conduct will come into force and be binding on every department/site/branch of the Company at the end of the grace period provided in Section 62(2) of PoPIA, which grace period will commence once the PoPIA commencement date has been affected in the Government Gazette If no grace period is granted, this Code of Conduct will come into effect and be binding on the COMPANY on the date that PoPIA or any proclamation by the State President requires compliance with those provisions.

9.2 Notwithstanding any delays in the commencement of PoPIA or the expiry of transitional arrangements stipulated in Section 114 of PoPIA, the COMPANY encourages its employees to ensure that the processing of personal information complies with PoPIA as early as may reasonably be achieved.

PART B – CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

10. GENERAL

10.1 PoPIA takes precedence over any other legislation that regulates the processing of personal information where that legislation is materially inconsistent with an object, or a specific provision of PoPIA, unless the other legislation regulates the processing more extensively than the conditions for lawful processing of personal information, in which event the more extensive provisions will prevail.

10.2 Chapter 3 of PoPIA stipulates the conditions for lawful processing of personal information. Codes of Conduct must incorporate these conditions or set out obligations that provide a functional equivalent to the obligations established in the conditions.

10.3 In considering the conditions for the lawful processing of personal information the separate conditions must not be considered in isolation. They should be regarded as a constellation of conditions that interact with and may influence the interpretation of the other conditions as circumstances

may dictate. For example: The purpose of collecting and processing personal information will impact on whether personal information is adequate, relevant, and not excessive and whether the processing of the personal information is justified. It may also impact on whether the personal information must be collected directly from a data subject and, depending on the scope of the initial purpose, whether further processing is compatible and permissible in terms of PoPIA. The Purpose specification may also influence the period for which personal information may lawfully be retained.

10.4 A further example is the requirement for Notification to a data subject where collecting personal information. This is inextricably linked to the provisions in other sections allowing a data subject to access personal information, require the amendment of incorrect personal information and object to the processing of personal information, all of which are dealt with in separate sections of PoPIA dealing with the conditions of lawful processing of personal information.

10.5 For the convenience of the reader the full text of each of the conditions for lawful processing of personal information are contained in this Code of Conduct. Definitions applicable to these provisions are also contained in the Definition section of this Code of Conduct.

10.6 The Company falls within the definition of “personal information” in PoPIA. In recognition of this PoPIA amends the Company to provide that Sections 68, 70(1), (2)(b) to (g) and (i), (3) and (4) and 72(1), (3) and (5) will be subject to the compliance procedures set out in Chapters 10 and 11 of PoPIA.

10.7 It must be noted that while the general principles of processing of personal information stipulated in PoPIA apply to all personal information, the Company shall retain its authority to deal with the filing of consumer/client/employee information.

10.8 The provisions governing the processing of information in the Company, while not as extensive as PoPIA, are not inconsistent with PoPIA and the Company complying in this regard will largely comply with the conditions for the lawful processing of personal information contained in PoPIA.

10.9 In consequence of their compliance the Company will, in many instances, have developed practices that comply with the conditions for the lawful processing of personal information or practices that constitute functional equivalence of what is required in these conditions. To the extent that it may be appropriate, guidance is provided relating to these practices and the correlation with the conditions for the lawful processing of personal information.

10.10 All persons that are subject to this Code of Conduct must comply with the conditions for the lawful processing of personal information stipulated in PoPIA.

11. CONDITION 1: ACCOUNTABILITY

Responsible party to ensure conditions for lawful processing:

11.1 The responsible party must ensure that the conditions set out in this section, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

11.2 Other Applicable Legislation:

11.2.1 In processing personal information, it is important that the Company establishes in what circumstances they act as responsible parties and in what circumstances they act as operators.

11.2.2 By definition a “responsible party” is a person who alone or in conjunction with others, determines the purpose of and means of processing personal information.

11.2.3 By definition an “operator” is a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party.

11.2.4 In processing personal information, whether as a responsible party or an operator must comply with the conditions for the lawful processing of personal information. The distinction lies in the fact that a responsible party is liable to the data subject and must ensure that all of the conditions of lawful processing of personal information and measures that give effect to these conditions are complied with. Specifically with regard to Security Safeguards in Condition 7, PoPIA requires that the responsible party must conclude a written contact with the operator and ensure that the operator establishes and maintains the security measures necessary to safeguard the integrity and confidentiality of personal information.

12. CONDITION 2: PROCESSING LIMITATION

Lawfulness of processing:

12.1 PERSONAL INFORMATION MUST BE PROCESSED:

a. Lawfully; and

b. In a reasonable manner that does not infringe the privacy of the data subject.

12.2 OTHER APPLICABLE LEGISLATION:

12.2.1 Aside from lawfulness, which would include the sharing of personal information for the purposes of the furtherance of the purposes outside the purpose of the Company, the person processing the information (this is not restricted to the responsible party) must ensure that it is processed in a reasonable manner so as not to infringe the privacy of the data subject;

12.2.2 What is “reasonable”? Reasonableness assumes that all of the conditions of lawful processing is adhered to;

12.2.3 Further, that the data subject has knowledge of:

a. Who is processing his or her personal information;

b. The intended use of the personal information; and

c. Can establish the manner in which the personal information will be handled and secured.

12.2.4 A data subject may reasonably expect that personal information will not be processed where the processing is unjustified or where it may have an unsubstantiated negative effect on the data subject.

12.2.5 If the Company processes personal information in compliance with PoPIA the processing will be lawful, reasonable and will not infringe the privacy of the data subject;

12.2.6 Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

12.3 PERSONAL INFORMATION MAY ONLY BE PROCESSED IF:

12.3.1 The data subject or a competent person where the data subject is a child consents to the processing;

12.3.2 Processing is necessary to carry out actions for the conclusion or performance of a contract;

12.3.3 To which the data subject is party;

12.3.4 Processing complies with an obligation imposed by law on the responsible party;

12.3.5 Processing protects a legitimate interest of the data subject;

12.3.6 Processing is necessary for the proper performance of a public law duty by a public body; or

12.3.7 Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

12.4 The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection 12.3 (a).

12.5 The data subject or competent person may withdraw his, her or its consent, as referred to in subsection 12.3.1), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection 12.3.2) to (12.3.7) will not be affected.

12.6 A data subject may object, at any time, to the processing of personal information**:**

a. in terms of subsection 12.3 (d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
b. (b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.

12.7 If a data subject has objected to the processing of personal information in terms of subsection 12.3, the responsible party may no longer process the personal information.

12.8 "Consent" means any voluntary, specific and informed expression of will in terms of which permission is given to the processing of personal information.

13. CONDITION 3: PURPOSE SPECIFICATION

Collection for specific purpose

13.1 Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;

13.2 Steps must be taken in accordance with section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18(4) are applicable.

13.3 Other Applicable Legislation:

a. In Section 68(1) of PoPIA any person who compiles, retains or reports any confidential information must protect the information and only use that information for the purpose permitted or required;

b. “Confidential information” is personal information that belongs to a person and is not generally available to or known by others;

c. Typically, personal information relating to a person’s financials or name, identity number, phone number, address etc. would be regarded by the data subject as confidential.

13.4 If the Company collects information directly from a data subject it must ensure that the data subject is aware of the specific, explicitly defined and lawful purpose related to the function and activity of the Company in processing the data subject’s personal information.

13.5 Retention and restriction of records:

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

a. Retention of the record is required or authorised by law;

b. The responsible party reasonably requires the record for lawful purposes related to its functions or activities;

c. Retention of the record is required by a contract between the parties thereto; or

d. The data subject or a competent person where the data subject is a child has consented to the retention of the record.

13.5.2 Records of personal information may be retained for periods in excess of those contemplated in 12.3 for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

13.5.3 A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must:

a. Retain the record for such period as may be required or prescribed by law or a code of conduct; or

b. If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

13.5.4 A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record.

13.5.5 The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

13.5.6 The responsible party must restrict processing of personal information if:

a. its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

b. the responsible party 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 data into another automated processing system.

13.5.7 Personal information referred to 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.

13.5.8 Where processing of personal information is restricted pursuant to subsection 13.5.6, the responsible party must inform the data subject before lifting the restriction on processing.

14. CONDITION 4: FURTHER PROCESSING LIMITATION

14.1 Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of Section 13 of the PoPIA;

14.2 To assess whether further processing is compatible with the purpose of collection, the responsible party 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 information has been collected; and

e. Any contractual rights and obligations between the parties.

14.3 The further processing of personal information is not incompatible with the purpose of collection if:

14.3.1 The data subject or a competent person where the data subject is a child has consented to the further processing of the information;

14.3.2 The information is available in or derived from a public record or has deliberately been made public by the data subject;

14.3.3 Further processing is necessary:

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

1.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

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

1.4 In the interests of national security;

1.5 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;

1.6 The information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

1.7 The further processing of the information is in accordance with an exemption granted under section 37 of the PoPIA.

15. CONDITION 5: INFORMATION QUALITY

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

15.2 In taking the steps referred to in subsection 14.1, the responsible party must have regard to the purpose for which personal information is collected or further processed.

16. CONDITION 6: OPENNESS

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

Note: Section 14 of the Promotion of Access to Information Act applies to public bodies and as the Company is by definition a private body in terms of that Act, Section 14 is not applicable and only section 51 is applicable.

16.2 OTHER APPLICABLE LEGISLATION:

The Promotion of Access to Information Act, 2 of 2000:

In Section 51 provides:

16.2.1 Within six months after the commencement of this section or the coming into existence of the private body concerned the head of a private body must compile a manual containing:

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

b. A description of the guide referred to in section 10, if available, and how to obtain access to it;

c. The latest notice in terms of section 52 (2), if any, regarding the categories of record of the body which are available without a person having to request access in terms of this act;

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

e. Sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject; and

f. Such other information as may be prescribed.

16.2.2 The head of a private body must on a regular basis update the manual referred to in Subsection (1).

16.2.3 Each manual must be made available as prescribed.

16.2.4 For security, administrative or financial reasons, the Minister may, on request or of his or her own accord, by notice in the Gazette, exempt any private body or category of private bodies from any provision of this section for such period as the Minister thinks fit."

16.3 A fundamental purpose of PoPIA is to allow the data subject access to and knowledge of his or her personal information that is being processed by either of, or both responsible parties and operators. Even if the data subject has knowledge through collection of the information directly from him or her or notification as required in Section 18 of PoPIA, if the information indicating how the personal information is being processed is not available to the data subject, he or she may be prevented from exercising the right to require amendment of inaccurate personal information or object to the processing of

personal information, as stipulated in PoPIA.

16.4 If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of.

16.5 The steps referred to in 16.3 must be taken:

a. if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or

b. in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

16.6 A responsible party that has previously taken the steps referred to in subsection 15.7 complies in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

16.7 It is not necessary for a responsible party to comply with subsection 16.3 if:

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

b. Non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this act;

c. Non-compliance is necessary:

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 as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

iii. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

iv. in the interests of national security;

d. Compliance would prejudice a lawful purpose of the collection;

e. Compliance is not reasonably practicable in the circumstances of the particular case; or

f. The information will:

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.

16.8 To enable data subjects to exercise their rights relating to the processing of their information a critical prerequisite is knowledge of the who, how and what relating to their personal information. Without this knowledge the data subject is deprived of the right to object to the processing of their personal information, prevent direct marketing, establish where automated decision-making may adversely affect them, and correct inaccurate personal information.

17. CONDITION 7: SECURITY SAFEGUARDS

17.1 A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

17.1.1 Loss of, damage to or unauthorised destruction of personal information; and

17.1.2 Unlawful access to or processing of personal information.

17.2 In order to give effect to section 17.1, the responsible party must take reasonable measures to:

17.2.1 Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

17.2.2 Establish and maintain appropriate safeguards against the risks identified;

17.2.3 Regularly verify that the safeguards are effectively implemented; and

17.2.4 Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

17.3 The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

17.4 NOTIFICATION OF SECURITY COMPROMISES

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify:

17.4.1 The Regulator; and

17.4.2 The data subject, unless the identity of such data subject cannot be established.

17.5 The notification referred to 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 responsible party's information system.

17.6 The responsible party may only delay notification of 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.

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

17.7.1 Mailed to the data subject's last known physical or postal address;

17.7.2 Sent by e-mail to the data subject's last known e-mail address;

17.7.3 Placed in a prominent position on the website of the responsible party;

17.7.4 Published in the news media; or

17.7.5 As may be directed by the Regulator.

17.8 The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

17.8.1 Description of the possible consequences of the security compromise;

17.8.2 A description of the measures that the responsible party intends to take or has taken to address the security compromise;

17.8.3 A recommendation with regard to the measures to be taken by the data subject to mitigate;

17.8.4 The possible adverse effects of the security compromise;

17.8.5 If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

17.8.6 The Regulator may direct a responsible party to publicise, in any manner specified, 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.

17.9 OTHER APPLICABLE LEGISLATION:

It is accepted globally that data subjects have the right to know if the security of their personal information has been compromised. It is the data subject who is best placed to protect him or herself against the abuse of their personal information but unless the data subject has knowledge of the compromise they are deprived of this right.

17.10 Financial information is by its nature valuable and is typically regarded as sensitive. This is illustrated by the fact that in Chapter 11 of PoPIA dealing with Offences, Penalties and Administrative Fines unlawful acts by responsible parties and third parties in connection with “account numbers” receive special attention.

THE COMPANY MUST:

17.10.1 Establish appropriate mechanisms to immediate notify the Regulator when reasonable grounds exist to believe that personal information of a data subject has been compromised;

17.10.2 Unless instructed to the contrary by the Regulator, as soon as reasonably possible, notify the data subject of its knowledge or suspicion that the data subject’s personal information has been accessed or acquired by an unauthorised person.

18. CONDITION 8: DATA SUBJECT PARTICIPATION

18.1 A data subject, having provided adequate proof of identity, has the right to:

18.1.1 Request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

18.1.2 Request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:

a. within a reasonable time;
b. at a prescribed fee, if any;

c. in a reasonable manner and format; and
d. in a form that is generally understandable.

18.1.3 If, in response to a request, personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.

18.1.4 If a data subject is required by a responsible party to pay a fee for services provided to the data subject to enable the responsible party to respond to a request, the responsible party:

a. must give the applicant a written estimate of the fee before providing the services; and
b. may require the applicant to pay a deposit for all or part of the fee.

18.2 A responsible party may or must refuse, as the case may be, to disclose any information requested to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply.

18.3 The provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records.

18.4 If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection 18.2, every other part must be disclosed.

Note: The Company is prohibited from processing health records and therefore the provisions of Section 61 of the Promotion of Access to Information Act is not applicable.

18.5 Correction of personal information. A data subject may, in the prescribed manner, request a responsible party 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 responsible party is no longer authorised to retain in terms of Section 14.

18.6 On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable:

a. correct the information;

b. destroy or delete the information;

c. provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or

d. where agreement cannot be reached between the responsible party 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.

18.7 If the responsible party has taken steps that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.

18.8 The responsible party must notify a data subject, who has made a request of the action taken as a result of the request.

18.9 Manner of access. The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of section 23 of this Act.

19. PROCESSING OF SPECIAL PERSONAL INFORMATION

19.1 Prohibition on processing of special personal information:

19.1.1 A responsible party may, subject to section 27, not process personal information concerning:

a. the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

b. the criminal behaviour of a data subject to the extent that such information relates to:

i. the alleged commission by a data subject of any offence; or

ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

19.2 The Company is expressly prohibited from processing information that correlates closely to the provisions of Section 26(a) of PoPIA.

19.3 Section 26 further prohibits the processing of personal information relating to criminal behaviour, in respect of which a data subject has not yet been found guilty of an offence. This is not directly addressed in the Company Regulations, but the Company does not process information of this nature.

20. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

20.1 A responsible party may not process personal information concerning a child.

20.2 General authorisation concerning personal information of children:

20.2.1 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.

20.2.2 The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

20.2.3 The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must:

a. Upon request of a competent person provide a reasonable means for that person to:

i. review the personal information processed; and
ii. refuse to permit its further processing;

b. Provide notice:

i. regarding the nature of the personal information of children that is processed;
ii. how such information is processed; and
iii. regarding any further processing practices;

c. Refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and

d. Establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

PART C – INFORMATION OFFICER, DIRECT MARKETING AND TRANSBORDER INFORMATION FLOWS

21. INFORMATION OFFICER

21.1 DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER

An information officer's responsibilities include:

a. the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;

b. dealing with requests made to the body pursuant to this Act;

c. working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;

d. otherwise ensuring compliance by the body with the provisions of this Act; and

e. as may be prescribed.

21.2 Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

21.3 DESIGNATION AND DELEGATION OF DEPUTY INFORMATION OFFICERS

21.3.1 Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of:

a. Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and

b. Any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

21.4 OTHER APPLICABLE LEGISLATION:

The Promotion of Access to Information Act, 2 of 2002 ("PAIA"):

a. PAIA, in relation to a private body, defines the head of a juristic person as the chief executive officer or equivalent officer of the juristic person, or any person duly authorised by the Chief Executive Officer.

b. In terms of PAIA it is the head or a person delegated by the head who acts on behalf of the organisation in fulfilling the organisation's obligations to provide access to records of the organisation;

c. PAIA will, on the commencement of the Act, fall to be regulated by the Information Regulator appointed in terms of PoPIA.

21.5 An Information Officer is defined in relation to a private body, which is a juristic person, as either the Chief Executive (or equivalent) Officer or the person duly authorised by the Chief Executive (or equivalent) Officer**.**

21.6 In the case of the Company unless the Chief Executive (or equivalent) Officer has appointed an Information Officer, the Chief Executive (or equivalent) Officer will be deemed to be the Information Officer.

21.7 PoPIA also stipulates that information officers must take up their duties only after the responsible party has registered them with the Regulator.

22. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATION AND AUTOMATED DECISION-MAKING

22.1 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, subject to subsection (3), a customer of the responsible party.

22.2 A responsible party may approach a data subject:

a. whose consent is required; and
b. who has not previously withheld such consent, only once in order to request the consent of that data subject?

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

22.4 A responsible party may only process the personal information of a data subject who is a customer /client/employee of the responsible party:

a. if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;

b. for the purpose of direct marketing of the responsible party's own similar products or services; and

c. if 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 marketing if the data subject has not initially refused such use.

22.5 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.

22.6 ‘‘Automatic calling machine’’, for purposes of subsection 21.1, means a machine that is able to do automated calls without human intervention.

22.7 Other Applicable Legislation:

The Consumer Protection Act, 68 of 2008 (“CPA”):

- The CPA deals relatively extensively with the right to fair and responsible marketing. This relates to all marketing of whatever nature and is not confined, as is the case with PoPIA, to direct marketing using electronic communications.
- The CPA deals with direct marketing to consumers in Section 32. This stipulates that where, as a result of direct marketing, a transaction is concluded for goods and services the consumer must be informed of the right to rescind the agreement. Further, that if any goods are left with the consumer without payment being made, the goods are to be considered unsolicited goods.

22.8 The principles governing direct marketing by means of unsolicited electronic communications are straightforward. There is no restriction on direct marketing by electronic communication to existing customers, provided that the customer is afforded the opportunity of opting out of further communications with the responsible party.

22.9 Where the data subject is not a customer, consent to the processing of personal information for the purposes of direct marketing (opt in) is required. The responsible party is entitled to approach the data subject for consent to direct marketing in electronic communications unless such consent has previously been withheld. If the person approached does not expressly agree to receipt of further electronic communications (opt in), any further communications to that person will be unlawful.

22.10 In terms of the Company the purpose of the processing of confidential information relates expressly to the provision of services that fall within the scope of the operations of the Company. If this information is used for another purpose such as direct marketing, this would be in breach of the Further Processing Limitations and unlawful.

22.11 Automated decision making:

22.11.1 A data subject may not be subject to a decision which results 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 basis of 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 reliability, location, health, personal preferences or conduct.

22.11.2 The provisions of subsection 21.11.1 do 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.

22.11.3 The appropriate measures, referred to in subsection 22.11.2 a. ii., must:

a. provide an opportunity for a data subject to make representations about a decision referred to in subsection 22.11.1; and

b. require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a).

22.12 Other Applicable Legislation:

22.12.1 The prohibition against automated decision making in the context of the operations of the Company, provided that a decision which may result in legal consequences for a data subject has been taken in connection with the conclusion or execution of a contract, and either:

a. The request of the data subject in terms of the contract has been met; or

b. Appropriate measures are in place to protect the data subject's legitimate interests in so far as automated decision making is concerned.

22.12.2 The protection of the legitimate interests of a data subject in this Code of Conduct is stipulated in Section 60(4)(a)(ii).

22.12.3 In addition to the reference to the protection of legitimate interests of data subjects in Section 71(2)(b) of PoPIA, the issue of legitimate interests of a data subject is addressed elsewhere in PoPIA.

22.10.4 Section 11(1) (dealing with the justification for the processing of personal information) stipulates that processing of personal information is lawful if it is:

a. Legitimate interests of the data subject;

b. Legitimate interests of the responsible party or of a third party to whom information is supplied;

c. Dealing with the collection of information directly from a data;

d. subject) provides that collection from another source is permissible if:

   i. The collection would not prejudice the legitimate interest of the data subject; and
   ii. Collection from another source is necessary to maintain the legitimate interests of the responsible party, or of a third party to whom the information is supplied.

e. In many instances the legitimate interests of both the data subject on the one hand or a responsible party or third party on the other, would coincide. However, this is not always the case and the necessity exists to balance the legitimate interests of the data subject with that of the responsible party or a third party.

f. In considering this balance it will always be necessary to take cognizance of the constitutional rights entrenched in the Bill of Rights of our Constitution. These rights are not absolute and any limitation to these rights have to be considered by taking into account the nature of the right, the important of the purpose of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose and whether there are less restrictive means of achieving the purpose.

g. Against this background where automated decision making is employed in the processing of personal information, a responsible party must, in protecting the legitimate interests of the data subject:

   i. Notify the data subject in terms of Section 18(1) that the processing of personal information may be subject to automatic decision making;

   ii. Provide to the data subject sufficient information about the underlying logic of the automated decision-making technologies and processes to enable the data subject to make representations relating to the decision automatically made;

   iii. Allow the data subject a reasonable opportunity for him or her to make representations to the responsible party about the decision.

23. TRANSBORDER INFORMATION FLOWS

23.1 A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless:

a. the third party who is the recipient of the 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 the 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 section, 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 responsible party, 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 responsible party 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. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

23.2 For the purpose of this section:

a. ''binding corporate rules'' means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

b. ‘‘group of undertakings’’ means a controlling undertaking and its controlled undertakings.

23.3 The purpose of prohibiting the transfer of personal information to a foreign country is straightforward. If the foreign country does not have adequate protection of personal information the possibility exists that the personal information (information knowing no borders) may be processed in a manner that violates the data subject’s right to privacy, including the right to determine the use of his or her personal information.

23.4 It is a feature of data protection legislation globally that unless the equivalent protection is provided in the foreign country, the transfer of the personal information to that country is prohibited, alternatively allowed subject to the fulfilment of conditions aimed to promote the protection of the personal information, regardless of the fact that there may be insufficient or inadequate laws in doing so in the foreign country.

PART D – ENFORCEMENT

24. INTERPRETATION OF POPIA AND THIS CODE OF CONDUCT

24.1 For the purposes of the interpretation of PoPIA and this Code of Conduct as well as the enforcement of PoPIA and this Code of Conduct “business days” shall mean all weekdays which are not proclaimed public holidays in the Republic of South Africa.

24.2 The Company or Executive Manager shall, for the purposes of this Part D of the Conduct of Conduct, include any person assigned by the Executive Manager to discharge the Executive Manager’s stipulated duties.

24.3 Consumers or Data Subjects

24.3.1 If customers/clients or data subjects (as defined in PoPIA) wish to complain about the conduct of the Company, PoPIA or this Code of Conduct the data subject must refer the complaint to the Company or the Information Regulator, as may be appropriate.

24.3.2 If a data subject is aggrieved with the actions of the Company on the grounds that they are contrary to this Code of Conduct, the complaint must be made to the Company or Information Regulator, as may be appropriate.

24.4 Interpretation and disputes relating to the Code of Conduct:

24.4.1 If a customer/client/employee of the Company wishes to request an interpretation of the Code of Conduct, the employee may address the

request or complaint in writing to the Executive Manager of the Company.

24.4.2 If the request cannot be resolved by the Company Executive Manager it will be placed on the agenda for discussion at the next meeting of Management meeting.

24.4.3 If, at the Management meeting, a request or a complaint cannot be resolved by the members attending the meeting, the Company Executive Manager must refer the request or complaint to the Company Executive Committee.

24.4.4 The Company Executive Committee may, in its discretion:

a. Make a decision and communicate the decision by email to its nominated representatives; or

b. Refer the request or complaint to legal counsel for consideration and opinion;

or

c. Recommend to the party requesting the interpretation or making the complaint to, at their own cost, obtain an opinion from legal counsel and provide this to the Executive Manager.

24.4.5 Once advice or an opinion has been obtained from legal counsel the Executive Manager will circulate this to the Executive Committee with a view to resolving the request or complaint.

24.4.6 If the party remains aggrieved by the advice or opinion from legal counsel, they may request the Company Executive Manager to again refer the matter to the Executive Committee, which may, but is not obliged to, appoint an independent adjudicator to consider and determine the request or complaint.

24.4.7 Nothing in this Code of Conduct prevents anyone from obtaining independent advice or opinion from legal counsel or a subject matter expert, as may be appropriate and providing this to the Executive Committee.

PART E – ADMINISTRATION OF CODE OF CONDUCT

25. COMPLIANCE WITH CHAPTER 7 OF POPIA

25.1 This Code of Conduct applies to the Company.

25.2 The Company has to apply to the Information Regulator for the issue of this Code of Conduct.

25.3 The Code of Conduct incorporates the conditions for the lawful processing of personal information and provides functional equivalence of obligations set out in those conditions that are applicable to the operations of the Company.

25.4 This Code of Conduct specifies appropriate measures for protecting the legitimate interests of data subjects with regard to “Automated Decision Making” in Part C.

25.5 This Code of Conduct will be reviewed by the Company within 1 (one) year of its coming into force in terms of Section 62(2) of PoPIA.

25.6 Further reviews of this Code of Conduct will be conducted annually by no later than the anniversary of the date of the coming into force of this Code of Conduct.

25.7 The review of this Code of Conduct may be accelerated:

25.7.1 if an earlier review is prescribed by the Regulator in writing addressed to the Company Executive Manager;

or

25.7.2 required in terms of a ruling made by the Regulator; or

25.7.3 if directed to do so by the Regulator in an Information Notice issued in terms of Section 90 or an Enforcement Notice issued in terms of Section 95 of PoPIA; or

25.7.4 if any court having jurisdiction over the Company who is a member of the COMPANY directs that any provisions of this Code of Conduct are unlawful.

25.8 The COMPANY will revoke or make any amendments to the Code of Conduct as directed by the Regulator, in compliance with Sections 60 to 63 of PoPIA.

25.9 This Code of Conduct will continue to be of force and effect indefinitely, subject to the Regulator’s direction as to the date of its expiry or termination by the Company.

25.10 On the termination of this Code of Conduct all employees of the Company will remain subject to the provisions of PoPIA and any other applicable laws governing the processing of personal information.

25.11 From the date that the Code of Conduct comes into force the Company will cause publication of the Code on its website.

25.12 The Company will make copies of the Code available in hardcopy form to persons requesting a copy in that form.

25.13 The interpretation of PoPIA and of this Code of Conduct as they relate to the operation of the Company may be made by the Company Executive Manager. No interpretation made by the Company Executive Manager shall be binding on the Information Regulator or detract from any of the powers of the Information Regulator stipulated in Chapter 10 of PoPIA.

25.14 The Company Executive Manager will ensure that a revision history of this Code of Conduct will be established and maintained.

25.15 The revision history must record the material aspects of any decisions or rulings made by the Regulator or by the Company Executive Committee that cause amendments to be made to this Code of Conduct.